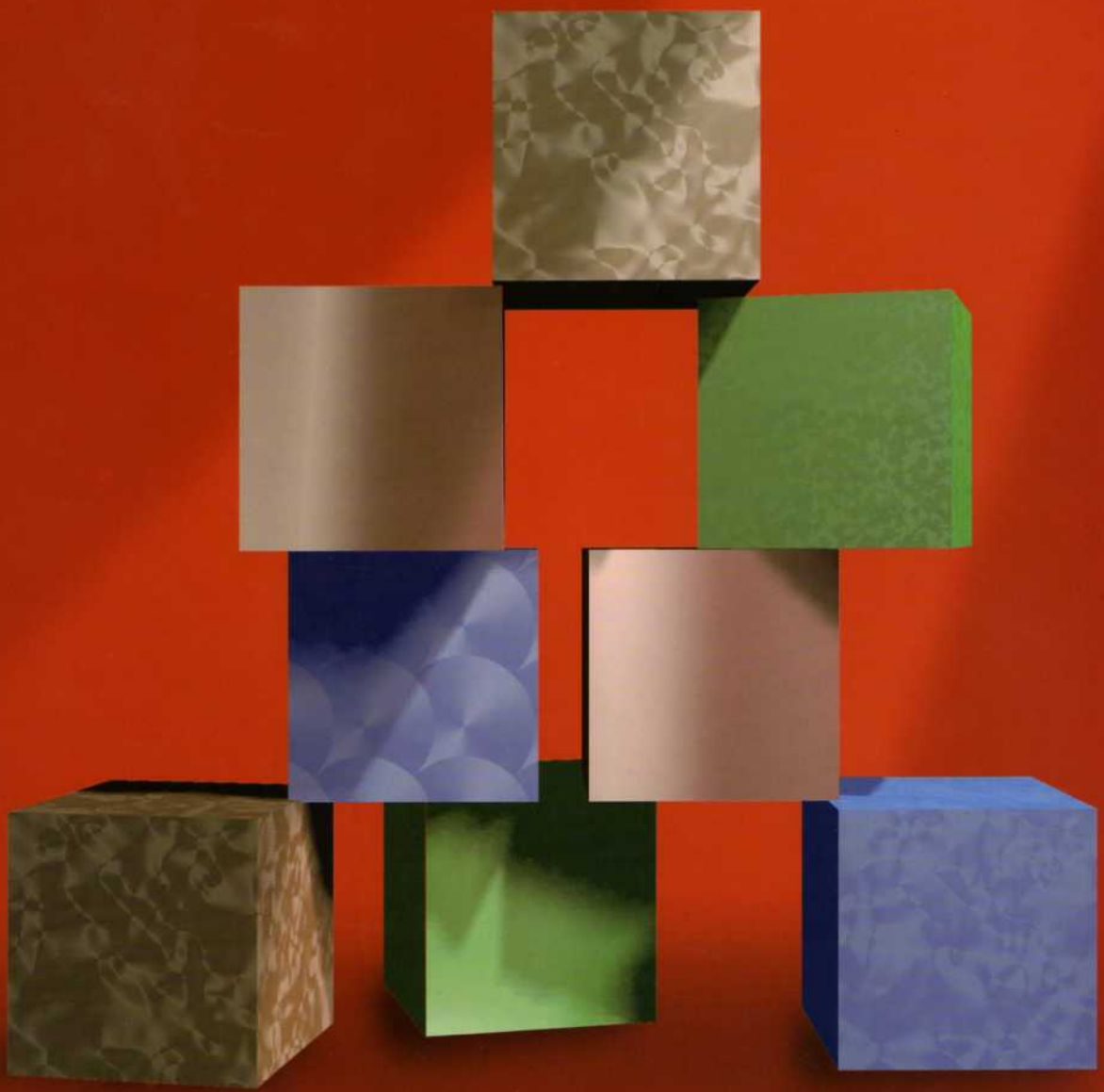
MANAGEMENT OF ENGINEERING RISK

Roger B Keey



IPENZ

CAE

Management of Engineering Risk

Roger B Keey
Professor Emeritus
University of Canterbury

with contributions from:
Geraint Bermingham
Don Houchen

Centre for Advanced Engineering, University of Canterbury

The Institution of Professional Engineers New Zealand

April 2000

ISBN 0-908993-25-0

First printing, April 2000

Editorial Services, Graphics and Book Design

Charles Hendtlass, Centre for Advanced Engineering

Cover

Design by Ken Hudson Design, Christchurch

Photographs

Inside front cover: View of the emergency construction of an overhead power line alongside the railway during the Auckland CBD electricity crisis in February 1998 as a result of the failure of four underground cables (see page 61 of text). Photograph courtesy of the *New Zealand Herald*.

Inside rear cover: View of the Opuha Dam collapse in February 1997 (see page 137 of text). Photograph courtesy of The Christchurch *Press*.

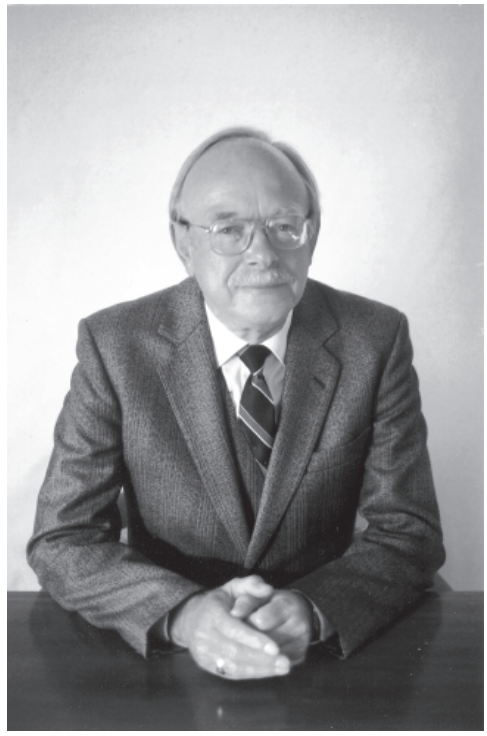
Printing

Wickcliffe Press, Christchurch

Disclaimer

This book has been prepared to assist professional engineers and others in the management of engineering risk, but does not purport to provide a standard or code of practice, neither does it set out to provide specific advice in any particular situation. The information in this book is given in good faith and belief in its accuracy, but does not imply the acceptance of any legal liability or responsibility whatsoever by the author, others who contributed, or by the Centre for Advanced Engineering or by the Institution of Professional Engineers New Zealand, for the consequences of its use or misuse in any particular circumstances.

JAN (JOHN) GARDENIER
1928 - 1999



This book is dedicated to the memory of John Gardenier, a member of the former Engineering Safety Committee of IPENZ, who tirelessly advocated the use of quantitative risk analysis.

Acknowledgements

The author and publishers acknowledge with gratitude assistance received from people and organisations in the preparation of this publication, and in particular:

- **The Consulting Engineers Advancement Society (CEAS)** for encouragement and financial support
- **Contributions to the text from**
  - **Geraint Bermingham,** Chapters 2 and 8, and material for other chapters as Principal Reviewer, including the provision of Case Study material
  - **Don Houchen,** Chapter 10
- **Reviewers of earlier draft versions of the text**

  On behalf of CEAS

  - Peter Smith, Dr Bill Wakelin and Geraint Bermingham

  On behalf of IPENZ

  - John Gardiner, Victor Lenting and the late John Gardenier

  Review of Chapter 9

  - Grant MacDonald, Partner, Phillips Fox Lawyers

The author and publishers wish to acknowledge the kind permission of the copyright holder to publish the following illustrations:

- The Institution of Chemical Engineers, Rugby (pp 41, 57, 82, 127)

We also wish to acknowledge with gratitude permission to publish Case Study material which has been provided by a number of organisations.

Foreword

Previous CAE Risk-Management Activity

The Centre for Advanced Engineering (CAE) has had a long-standing interest and involvement in risk-management issues. In its first major project leading to the August 1991 publication, *Lifelines in Earthquakes: Wellington Case Study*, engineering-risk management issues were an important consideration in relation to the ongoing functioning of essential infrastructure and services following a major earthquake. The subsequent multi-hazard Christchurch Engineering Lifelines Project, in which CAE was also involved, led to the November 1997 publication entitled *Risks and Realities*. Another early CAE publication in October 1992 , *Risk Assessment of Industrial and Natural Hazards,* was edited by the late Mr John Gardenier and by Professor Roger Keey with contributions from 16 practitioners.

Other CAE publications, where risk-management issues in engineering have been an important consideration, have included:

- Waste Landfill Engineering Guidelines;
- Treatment of Hazardous Waste;
- Reliability of Electricity Supply; and
- Fire Engineering Design Guide.

In March 1997, CAE organised a very successful two-day conference in Wellington on Integrated Risk Management followed up by a one-day conference in Auckland in November that year, leading to the publication, *Owning the Future,* launched at Parliament in September 1998.

Further information on CAE is given in Appendix C.

Background to the Production of this Publication

The original idea for a book on *Management of Engineering Risk* came from my attendance at a February 1996 NZ Geotechnical Society conference in Hamilton on "Geotechnical Issues in Land Development". I represented IPENZ at that conference to present proposals then being mooted for the establishment of Practice Colleges within the Institution. Several times during discussions at the conference, the 1983/84 IPENZ publication on *Engineering Risk* was mentioned by people who had found it to be helpful in their professional practice.

At the time of its release, this 1983/84 publication was distributed free of charge to all members of the Institution and I remembered that I still had a copy on my bookshelf. On my return home I re-examined it and reached the conclusion that the production of a revised and updated version would be an appropriate project for CAE.

I then approached both IPENZ and the Consulting Engineers Advancement Society (CEAS) who had supported the original 1983/84 publication, with the proposal of us-

ing it as the basis for a new updated publication on engineering-risk management. Both organisations offered support and financial assistance for the project.

Professor Roger Keey of the University of Canterbury was then approached, and after discussions extending over several months leading to the development of a proposed scope for the project, he agreed to prepare a draft text of such a publication for review. The first draft was produced in September 1998. The review was then carried out by both IPENZ and CEAS. Subsequently Mr Geraint Bermingham was engaged by CAE as principal reviewer. He has provided most valuable assistance in the preparation of the final text and his contribution is gratefully acknowledged.

The publication of the Australian/New Zealand Standard on Risk Management (AS/NZS 4360: 1995) and its reissue in revised form in 1999 was also an influencing factor in the preparation of this publication, which can be seen as an engineering-related "companion volume" to the Australian/New Zealand Standard.

Recent Major Incidents

The February 1997 collapse in a flood during construction of the Opuha Dam in South Canterbury, followed a year later in February 1998 by the Auckland CBD electricity crisis helped to raise general awareness within the profession in New Zealand of the importance of understanding issues in engineering-risk management. Soon after, there were two major incidents in Australia; quality problems with drinking water in Sydney and an explosion leading to a state-wide disruption to the natural gas supply in Victoria. This again raised awareness and highlighted the importance in all engineering activity of implementing good risk-management procedures to help prevent such incidents happening in the future, with consequent inconvenience to the public and adverse publicity. The continued functioning of a modern society has become highly dependent on technology.

Such incidents emphasise the importance to many professional engineers of implementing appropriate risk-management procedures on projects for which they are responsible, even if the impact and scale of a potential failure is of a much lower order than the incidents described above. I hope that many members of the profession will find this publication to be helpful to them in handling risk-management issues in their everyday working lives.

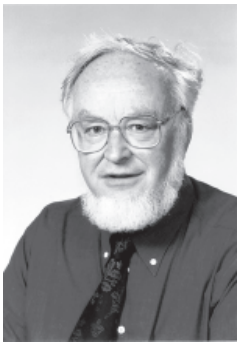
Appreciation

I would like to express my own personal appreciation to Professor Roger Keey for the tireless application of his own professional knowledge and skill over several years to bringing this project to a successful completion, with the assistance of a number of individuals and organisations whose help is also gratefully acknowledged.

John Blakeley

CAE Executive Director (1988-2000)
Past-President of IPENZ (1997-1998)

April 2000



Preface

Most of us will live longer, healthier and safer lives than our parents or grandparents. Yet we still worry about threats to our well-being. The public awareness of engineering risk has been raised recently by several major incidents in both New Zealand and Australia. We expect better reliability in our modern technological society.

Eric Ireland, on becoming President of the Institution of Professional Engineers New Zealand (IPENZ) in 1983, set up a task committee to study the subject of engineering uncertainties and risks and to prepare a publication on the subject that would be a suitable reference for the engineering profession and those associated with it. The incentive for such a work was summarised in a quotation from a collection of essays on "Engineering and Society" (Hayward 1982):

> *"Throughout the centuries our standards of living and quality of life have been profoundly influenced by engineering endeavour. The irony is that with each accomplishment, society's expectations have been raised and its perceptions of human welfare altered."*

Since the publication of the book *Engineering Risk* by the task committee (Strachan et al. 1983), the commercial, professional and statutory environment in which professional engineers must work has changed considerably. While the 1983 book was well received by the engineering profession, clearly its contents have now been overtaken by subsequent events. In March 1996, IPENZ accepted a proposal that the 1983 book should be updated in a joint publication with the Centre for Advanced Engineering (CAE) at the University of Canterbury. The Consulting Engineers' Advancement Society (CEAS) generously offered sponsorship towards the cost of the publication and provided advice on the content of the revision.

The original work was written by a number of contributors, but it was decided that the revised work should have the greater coherence provided through a single authorship. Professor Roger Keey, whose book "*Safety and Reliability in the Process Industries*" had already been published earlier by the Institution in 1987, was approached to do this revision. He also had been a member of an Australian/New Zealand Standards Committee which had developed a generic standard on risk management (AS/NZS 4360:1995).

To ensure an adequate perspective in the revised work, the text was initially read by representatives of CEAS and IPENZ, and reviewed by Geraint

Bermingham, a specialist in engineering-risk management. After the first draft was prepared, and after consultation with both IPENZ and CEAS, it was decided to change the focus from a revision of the 1983 work to a new work, being more of a guide for the members of the engineering profession to the template of AS/NZS 4360:1999, which should be seen as the definitive document for managing risk in Australia and New Zealand. At the same time, in early 1999, IPENZ issued a policy statement entitled "*Risk and Prudence*" on risk and governance in public and private organisations that rely intensively on engineering and technology in their activities or business (see Appendix B).

Geraint Bermingham was appointed by CAE to provide a peer review of the new work. He also substantially prepared the writing of a new chapter on an overview of engineering-risk management, the framework for a chapter on workplace risk, and provided material for other chapters. Don Houchen of Aon Risk Services Group kindly provided text for the chapter on risk insurance.

The author is grateful for the constructive comments in the various reviews in the attempt to achieve a balanced, introductory work for use by engineers, engineering managers and their associates. His viewpoint is from one who now has a degree of detachment from the workface of engineering-risk management. Others may see the same topic from different aspects. Furthermore, a greater maturity of understanding about the nature of engineering risk since the publication of the 1983 report of the IPENZ task committee has not always led to greater consensus, as illustrated in the Report of the Study Group commissioned by the Royal Society of London in 1991, to update its own 1983 Report on Risk Assessment which was more straightforward in describing risk assessment.

A fairly short book on the subject cannot be comprehensive (the literature is advancing at the rate of 500 major publications per year), nor it is designed to be a prescriptive handbook on engineering-risk assessment, nor a detailed manual for risk management. However, the book does provide an overview of the strategy and techniques of engineering-risk management, while a selected range of references enables the reader to follow up particular aspects in greater detail and gain some insight into the benefits of this approach Thus, it is hoped that this new work will be useful to the engineering profession and others wishing to implement a risk-management approach within their own organisation or project, as a "companion volume" in providing an introduction to the application of the Australian/New Zealand Standard AS/NZS 4360:1999, and a first guide to engineering risk, its perception, identification and evaluation, which forms a basis for the prudent management of engineering assets and operations.

Roger B Keey
Christchurch

December 1999

Contents

Case Studies

1 Introduction

Engineering risk arises from uncertainty. This may be due to incomplete knowledge or understanding, to the appearance of unforeseen events that may be of commercial, political or social origin, or to an inability to control a developing situation. Such events, if they happen, may result in loss or harm to people, property and the environment. Even when risks are reduced, avoided or transferred, there is always some residual chance that things may go wrong, occasionally badly wrong.

We normally think of a risk being the chance that some adverse thing might happen of the consequence should it do so. Specifically, with engineering risk, we mean the practical likelihood of a specific hazard being realised through engineering activity given the actual workplace practices, management priorities, constraints and pressures[1]. Taking risks, however, may lead to gain, and this anticipated gain is normally the incentive for undertaking risky ventures.

Indeed, absolute safety is an impossible dream. Even doing nothing is risky. Many lives were lost in fording New Zealand rivers before they were bridged. Yet our attempts to overcome such risks often bring others we may not have considered. Bridges can and do fail. Further, we cannot even say that the only perfectly safe bridge is the one that has not been used. The collapse of the Westgate box-girder bridge under construction at Melbourne, and the destruction by fire of an Apollo spacecraft on the launching pad both illustrate that failures can occur before things are used for their designed purpose. The management of risks throughout the complete lifespan of a project from initial conception onwards is thus an important aspect of modern business and engineering enterprises.

Although a lack of safety can lead to tragedy, there is sometimes a comic side to relieve its seriousness. Smith[2] relates the story of a sphere which normally held liquid propane and was being filled with water to expel any oil vapours. Unfortunately, the supporting legs could not stand the weight, water being heavier than oil, and the sphere fell over. A mobile crane was brought to raise the sphere, but the crane's jib could not withstand the load, and collapsed sideways over the sphere, causing further extensive damage.

Considerable effort has been expended in recent decades to devise ways of assessing and monitoring risks to put a measure on their real value, so that we can minimise or avoid the major ones, leaving untreated the minor ones of little consequence that we may be prepared to live with, at least for the time being. While such techniques have yielded demonstrable progress in a reduc-

tion of accidents and increase in safety, perceptions often remain that technological risks are too great and increasing.

The reality of a risk does not derive simply from such so-called "objective" measures. Newby[3], in his address for the 1997 Jubilee Lecture of the Institution of Chemical Engineers in London, quotes the word of an American social psychologist, W I Thomas:

> *"Things which are perceived as real will be real in their consequences"*

We perceive risk through the accumulated wisdom of our forebears and our own experience and those of the society in which we live. Such informal measures were adequate when society was relatively static and new experiences were rare. While there is little doubt that the world is a healthier and safer place for most of its inhabitants than a century ago, there is more uncertainty through seemingly ever-increasing rates of political, social and technological change. These changes, noted Newby[3], have left individuals feeling threatened with a sense of greater unpredictability and increased vulnerability. The past is no longer a simple template for the future. Moreover, few in society unquestioningly believe that our pursuit of new knowledge and gain of new skills will bring about human progress and happiness. This loss of confidence has its expression in an enhanced perception of risk and a suspicion of expert opinion, with the rise of independent groups presenting alternative viewpoints.

The perception of risk is a social belief. A proposed medium-density fibreboard plant in the Dunedin area did not gain a resource consent because of the perceived risks of emissions, even though the quantitative assessment showed these risks to be minor and their long-term environmental impacts to be negligible. *The thing that was perceived to be real was real in its consequenc*e. Real are the perceptions of the risks of living near high-tension power lines, of irradiating food, of the introduction of genetically-modified organisms, or even of the visits of nuclear-powered warships. Such perceptions do influence political and social policy, and ultimately shape the pattern and pace of technological change, regardless of technical measures of risk. *Today, the communication of risks can be as important to a successful outcome of an engineering project as the treatment of the actual risks.*

Within business and commerce, risks usually will be measured in monetary terms. Even here the perception of risk and the perceived effect of failure on the corporate image can be as important as financial estimates.

Just as individuals and organisations set themselves personal thresholds of tolerable risk, so too communities develop informal but real perceptions of thresholds of societal risk[4]. Accidents and failures that cause large-scale damage or

multiple fatalities are almost always followed by a public outcry, often leading to some kind of inquiry into the cause and the steps needed to prevent a re-occurrence. We are risk-averse, particularly whenever the risky venture is outside our control. As a society, we appear to seek the elimination of high-severity risks that might be experienced in an average lifetime.

Risk perception involves a range of social and cultural values and attitudes towards hazards and their benefits. Different people will perceive a given risk differently, depending on their value systems they hold and the benefits they derive, and view it within different contexts. Thus it is impossible to reduce the perceived risk into a single objective function, such as a mean probable fatality rate, or some product of likelihood and consequence. The human condition is of wider compass.

This does not mean that quantitative measures of engineering risk are useless, and the assessment and control of hazards should be left to adversarial debate in resource consent hearings or the judgement of the Environment Court. Rather, the reality of so-called "objective" risk assessments has to be set alongside the reality of perceived risk in formulating policy. Engineering-risk assessments play a vital role in the wise use of resources and in the development of a project from its conception to its "death". Only by quantitative measures can we ascribe priority to alternative risk-reduction strategies or monitor improvements in safety, health and the environment.

Elms[5] has written:

> *"Engineering is goal-oriented, rather than truth-oriented ... in that it has an end in mind."*

Engineering has often regarded the end in providing for society's perceived needs as justifying the means, but no longer is that the case. The IPENZ Code of Ethics now looks towards sustainable management and care for the environment with minimal adverse side-effects. Consideration of means and the evaluation of associated risks at all stages of a project are thus essential components of engineering endeavour.

The incentive for writing the original IPENZ book was a growing concern for the liability of engineers in an increasingly critical and litigious world. The then President of the Institution, Eric Ireland (1983-4), noting that some spectacular failures had figured prominently in newspapers or had been featured on television, appointed a task committee to study the subject of engineering uncertainties and risks and prepare a publication that might be used as a reference for the engineering profession and those associated with it. Their work set out to review the nature of engineering risk. To address the particular concern with liability, the publication contained several appendices dealing with matters of

law and insurance which were prepared by professional advisers to the editorial committee.

Since the publication of that book, as noted in the Preface, the commercial, professional and statutory environment in which professional engineers work has changed considerably. The aggregated body of engineering expertise within the former Ministry of Works and Development has been dispersed; the corporate heirs of the old NZ Electricity Department and Post Office have much leaner in-house infrastructures. The Building Act (1991) and its Regulations (1992) are an example of newer legislation that is outcome-driven, rather than prescriptive in content. The Resource Management Act (1991) has introduced the concept of sustainable management of resources and placed a duty on both principals and employees to avoid, eliminate or mitigate "effects" on the environment. The definition of effects is very wide in the Act, covering both acute and long-term impacts, whether remote or not and whether of short duration or not. Subsequent legislation, such as the Health and Safety in Employment Act (1992) and the Hazardous Substances and New Organisms Act (1996), with the setting up of the Environmental Risk Management Authority in 1998, now provide a new statutory framework for engineering activity beyond the traditional obligation of an engineer to practise her or his profession with reasonable and proper care and skill.

A number of recent infrastructural failures in New Zealand and Australia has also raised concerns about the prudent management of engineering assets and operations. In early 1999, the President of IPENZ, Sir Ron Carter, issued a policy statement entitled, *Risk and Prudence*, on behalf of the Institution (see Appendix B). This statement provides guidelines for organisations that rely intensively on engineering and technology and for which engineering-related risks are a significant proportion of the total risk of conducting business. It recommended that organisations should ideally have at least one Board Member with a recognised professional engineering background. In executive management, there should be a person or persons (as appropriate) having clear responsibility and accountability for engineering and technology matters, with engineering risks being properly evaluated and considered in assessing the overall business risk. Within an organisation's business activity, there should be a regular audit of performance of its engineering policies, including those applying to engineering personnel, measured against industry's "best-practice" standards. The statement concludes by noting that adherence to the proposed policy would help those with responsibilities for governance to show that they have acted prudently in managing the engineering resources entrusted to them.

The 1983 report of the IPENZ President's task committee set out a number of conclusions and recommendations, many dealing with aspects of engineering liability. The thrust of these earlier conclusions reflected the concerns of the task committee, with its engineering members drawn from the ranks of consult-

ing and public works engineers. Subsequently, the Institution has declared, within its revised Code of Ethics, that its members' concern for risk has a wider compass. Engineers have a duty of care to protect life and safeguard people. Specifically, members are required to:

1. **Give priority to the safety and wellbeing of the community and have regard to this principle in assessing duty to clients and colleagues;**
2. **Be responsible for ensuring that reasonable steps are taken to minimise the risk of loss of life, injury or suffering which may result from the work or the effects of a member's work;**
3. **Draw attention of those affected to the level of significance of risk associated with the work;**
4. **Assess and minimise potential dangers involved in the construction, manufacture and use of a member's products or projects.**

The Code also specifies that members shall be committed to the need for sustainable management of resources and seek to minimise adverse environmental impacts of engineering works or applications of technology for both present and future generations.

At the same time, there has been a greater awareness of the need for integrated risk management, in many fields besides engineering, culminating, for example, with the publication of the Australian/New Zealand Standard AS/NZS 4360:1995, and its reissue in revised form in 1999. Further examples of the increasing importance placed on this approach to management include the holding of the Wellington conference in March 1997 on *Integrated Risk Management* under the auspices of the Centre for Advanced Engineering and the issuing of a statement of policy on *Risk and Prudence* in engineering governance by the IPENZ Board, which has been already referred to. It seems appropriate, then, in this book to provide both an overview of the management of engineering risk as well as a more detailed treatment than its predecessor on the nature of engineering risk, its identification, analysis, evaluation and treatment, including the impact of recent legislation on professional engineering practice as a result of political and social perception of risks to persons and the environment from engineering works. The book is thus more of a first guide to the topic of managing engineering risk, written to the template of the revised Risk Management Standard AS/NZS4360:1999, rather than a review of the liability of engineers from the risks they run in the exercise of their profession.

Engineering-risk management is concerned with mechanisms of recognising and facing threats to a technology-based organisation before they have a chance to inflict expensive and possibly irreparable damage. These threats may have a technical origin, but normally the prime cause is poor management of engineering processes and facilities.

References

1 Blackmore, G A and Shannon, H D (1996): "Risk-based safety-management auditing", *Process Safety and Environ. Protection,* 74(B1), 38-44.

2 Smith, M (1998): "Safety can be fun", *IChemE Loss Prevention Bull.*, No. 139, 2.

3 Newby, H (1997): "Risk analysis and risk perception: The social limits of technological change", *Proc. Safety & Environ. Protection,* 75 (B3), 133-7.

4 Helm, P (1997): "Risk assessment, methodology, vulnerability, impact and importance", in Rep. Christchurch Engineering Lifelines Group: "*Risks & Realities*", CAE, Univ. Canterbury, Christchurch.

5 Elms, D G (1992): "Risk assessment" in D J Blockley (ed.) "*Engineering Safety*", McGraw-Hill, New York.

2 Management Overview*

Risk-based Approach

Engineering activities involve uncertainties of various kinds. Risk management is concerned with coping with these future uncertainties, by planning for the unintended outcome, through avoidance or mitigation should it happen, thereby reducing future losses. Indeed, *loss prevention* is the term sometimes employed for risk management.

Elms[1] distinguishes between management *of* risk and the management *with* risk. The management of risk is concerned with reducing the risks faced by an organisation and maintaining them within acceptable limits. For this, one needs to understand methods of risk reduction; the risks may not need to be quantified precisely, but ranked in priority for treatment. Management with risk, on the other hand, typically is associated with business risks. For a company to grow, investments must be made, and there always is a risk associated with them. Proper management quantifies this risk as precisely as possible so that the venture can proceed with confidence. Engineering risks normally encompass both kinds of risk management.

Risk management does not imply *constrained* management, for an organisation that does not take risks is probably at higher risk of ultimate failure than one that seizes opportunities despite the attendant risks. Innovation normally involves risks, and sometimes leads to spectacular failures. In the late 1940s, the first *Comet* commercial jet airliners were designed without full knowledge of fatigue-stress development. Failures in service had high costs in human and material terms. However, a process of systematic risk identification and assessment allows organisations to understand the risks inherent in a course of action, to be informed of potential failures and to have a basis to prepare contingency plans, thereby reducing the consequences of any mishaps. *This process requires the active involvement of senior executive management of technological enterprises, who should ensure that engineering risks are properly considered in evaluating their business risks*. The following chapters outline some of the risk-management tools which can be used by those concerned with the built environment and with the development and use of technology.

Driving Forces

There are a number of factors that are leading to the rapid adoption of risk-based management. There is an increasing awareness of its benefits as a means

*** based on original text by Geraint Bermingham**

of reducing future losses, while achieving a balance between the risk of failure and the reward of success. Managers are working in an increasingly complex and global environment, under rapidly changing conditions, and the risk of business activity is a central element of corporate governance.

Societies have increasing expectations regarding their own wellbeing as well as of corporate responsibilities. As noted in Chapter 1, recent well-publicised failures of engineering services and works has led the Board of IPENZ to issue guidelines on governance of organisations that rely on engineering and technology.

The enhanced expectations are reflected in recent legislation. The Consumer Guarantees Act 1993 sets out the responsibilities of those providing goods and services. Both the Commerce Act and the Health & Safety in Employment Act 1992, place statutory requirements for compliance with legislation to show that managers have acted prudently and have followed best practice, to reflect society's expectations of wellbeing and corporate responsibilities. The Building Act 1991 focuses on the risk to users of buildings and those involved in emergency actions following incidents within them. As a result, the Building Industry Authority has commissioned a number of risk studies as well as a generic risk-model. This model requires all risk projects carried out by or for the Authority to conform to a set framework and to meet certain criteria and standards.

Another recent development has been the setting up of the Environmental Risk Management Authority (ERMA). For all applications under the Hazardous Substances and New Organisms Act 1996, each type of hazard, which could arise from the introduction of a hazardous substance or new organism, will be assessed for the type and level of risk posed.

At local level, the granting of resource consents under the Resource Management Act 1991 increasingly require the applicants to carry out a formal risk assessment of the undertaking in question to determine its likely effect on the environment. Although consenting authorities appear to be moving towards the use of risk-based standards of performance, there are no formal criteria for deciding what is safe. Authorities have tended to bring down conservative decisions influenced by earlier deterministic requirements, as the history of the consent processes for liquefied natural gas storage facilities has illustrated. The full benefits of the use of risk-based standards has yet to be obtained.

Business Issues

Risk is often conceived as the flip side of opportunity or gain. In business, this is often true, although these two aspects of a course of action are often not directly linked. Armed with a good understanding of risks, it is usually possible to reduce these without restricting the available opportunities. Even a sim-

ple awareness of all the risks can be enough to contain and reduce them, and thus tip the balance of an activity towards reward. Risk management is a key element of any organisation. *Failure to put in place some appropriate form of risk-management protocols and procedures within the organisation is now viewed negatively within business circles and by investors.*

Organisations tend to hide unpleasant news, with the causes of failure obscured by management. Investigations need to delve deeply, particularly when the risks seem to be high or uncertain. Companies have often paid dearly after suffering an incident they were not prepared for or had not put appropriate resources into mitigating. The costs of not carrying out a formal systematic review of one's risks and then implementing suitable risk-reduction policies and procedures can be high.

On the other hand, large savings can be achieved, as claimed by one Californian brewing company that implemented a risk-reduction programme prior to the incidence of a large earthquake which would have resulted in a substantial loss if no action had been taken[2]. The company is reported to have saved over US$750 million as a result of spending US$17 million on a risk reduction programme implemented before the 1994 Northridge earthquake. No major injuries were suffered by their employees and they were, unlike the surrounding industry, back in full production within seven days.

Formal Risk Management

All those in positions of management, whether they are aware of it or not, are making qualitative risk-based judgements every day. Without formal risk training, most of these decisions will be skewed towards avoidance of incidents of high consequence or those likely to be known or have been seen. The extent of risk-taking would depend upon a person's natural level of aversion and philosophy.

However, it is now possible to be systematic and consistent, thus improving the chance of identifying the unexpected. Being consistent allows rational decision-making over time and across an organisation's structure. For large organisations, with a number of sub-structures, this last point is important as many aspects of risk, such as technical, financial, insurance and political issues, need to be considered.

Risk management is an ongoing aspect of good management and needs to be integrated into the activities of the organisation. The management of risks should not be seen as a simple one-off activity in which some risk consultants come in, set up a risk register, quote from some standard or text, and then depart. *Effective risk management takes continual effort in developing a culture in which people are trained to think about risk in making decisions*; the risk analysis must be thorough, responses to events and crises need to worked out,

and standard emergency and contingency plans need to be put in place. An organisation's risk profile will change over time, so the risk management needs to be live, ongoing and aware of developments, often under the guidance of a risk committee. Case Study 2.1 describes an example of effective risk management. (An analogous series of events occurred in the failures of the electricity supply to Auckland's central business district in early 1998.)

Case Study 2.1 Reliability of a Power Supply (Bermingham, 1999 *pers. comm.*)

A failure of one of a number of important power supplies to a large industrial site led to a meeting of the site's risk management committee. Based on the high risks associated with further failures and the yet-unknown causes, it was decided that, despite the significant disruption to customers and the attendant risks, all other supplies would be limited to 80% full load. This was considered necessary as, until investigations proved otherwise, the root cause of the failure could be common to all the supplies.

In the event, the root cause of failure was soon found to be associated with a new type of overload trip fitted to most of the supply transformers, which could not cope with a recent long period of unusually warm weather. Transformers fitted with the older type of trip were immediately cleared for full-load operation, and the others only after modification and testing.

In the absence of knowledge coming from earlier formal risk studies and appropriate emergency operating procedures for this type of event, the site's management might have decided to maintain full load on the other supplies. This policy would have been dictated by the requirement to meet the customer's immediate needs, thus increasing the chance that these units would have failed subsequently with the progressive degradation of the whole system. A lack of understanding would have hindered the management of the event.

This example demonstrates that a risk-based approach to management can reduce the risks associated with failures by forearming the operators and decision-makers with the knowledge to *react correctly to failures*, as well as to mitigate to prevent them.

Consultants do have a role in bringing fresh eyes into an organisation, and helping update current risk-management structures. They are good for auditing peer-review roles, as well as being involved in novel and one-off studies. However, when they leave, the organisation needs to have an ongoing structure flexible enough to serve for the years to come in a rapidly changing business environment.

Risk management, like any tool, can be abused. It is not a matter of measuring risk, using a formula to decide whether something is safe or not, of slavishly obeying a prescription. *There is no such thing as absolute assurance or safety. Things can and do go wrong; losses will be suffered. The future cannot be predicted, but bets can be hedged.*

Risk Identification, Assessment and Treatment

An organisation cannot seek assurance through ignorance, on the grounds that

it is better to be unaware of risks than to treat them. Ignorance is no defence and the Health and Safety in Employment Act 1992 requires employers to ensure that there are effective methods for systematically identifying, assessing and reducing hazards in the workplace. Moreover, the Resource Management Act 1991 requires that organisations put in place good environmental practices, which demand the identification and treatment of risks.

Any organisation is constrained by available resources. A proper risk assessment, however, enable the risks to be systematically ranked, and tackled in a logical order to drive down the total risk as quickly and as effectively as possible. The goal is to achieve *continuous improvement* in risk identification, assessment and treatment.

If the organisation has a risk-management plan and is implementing it within all practical limitations, then this is a suitable defence if an accident does happen. The principle, *As Low As Reasonably Practical (ALARP),* is now the accepted underpinning of much legislation.

Standards

The Australian/New Zealand Standard AS/NZS 4360:1999 *Risk Management* provides a *generic guide* for the establishment and implementation of a risk-management process. This involves establishing the context and identifications of the risks, their analysis, evaluation, treatment, communication and ongoing monitoring. Risk management is recognised by the Standard as an integral part of good management practice. It is an iterative process consisting of steps, which, when undertaken in sequence, enable a continual improvement in decision-making to take place. The whole process of risk management, then, can be depicted within quadrants of risk identification, analysis, evaluation and treatment, as illustrated in Figure 2.1.

Another view, Figure 2.2, illustrates that risk communication is central to this process and takes place in all stages. The advantage of this generic Australian/New Zealand Standard is that it provides a structure that all professions can relate to. Those interested in finance, insurance, the environment or technology within a given organisation must speak the same language and work within a common reference frame which enhances communication. Use of this Standard as a template for management enables this to be done.

The publication of the AS/NZ 4360 in revised form in 1999 was predated by the appearance of AS/NZS 3931:1998 *Risk analysis of technological systems - Applications Guide*, the object of which is to provide guidelines for selecting and implementing risk-analysis techniques. It also gives a useful summary of the established tools relating to technical safety and reliability analysis, but does not give detailed prescriptions of how such analyses should be carried out.

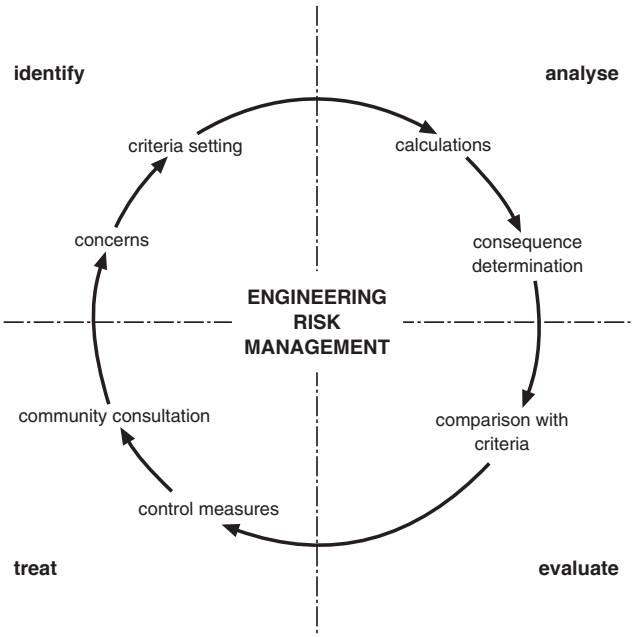


Figure 2.1: The "seven seas" of engineering-risk management (after Beer 1998, pers. comm., with modification)

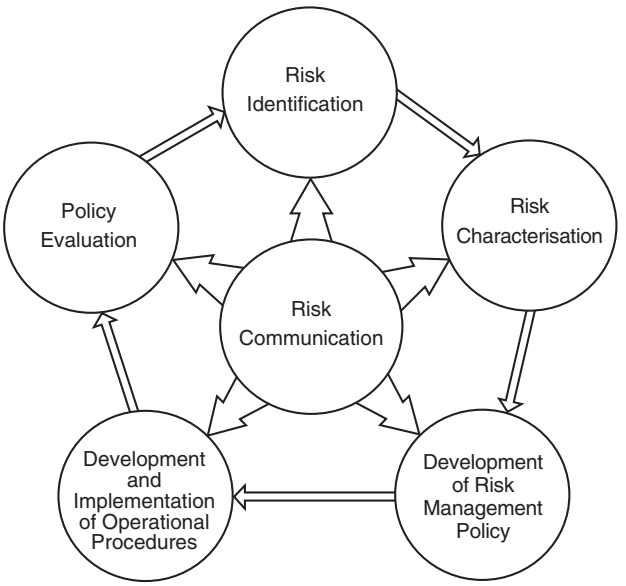


Figure 2.2: The centrality of risk communication (Bermingham, 1999 pers. comm.)

At the time of writing in late 1999, an Environmental Risk Management Guide was being prepared by a joint Australian/New Zealand Standards Committee to provide an explanation of how the generic Standard can be applied to develop environmental risk-management policies. This Guide notes that environmental risks can be grouped into two types: the risk to the environment from the activities of an organisation; and the risk to the organisation from environment-related issues, including the risks of non-compliance with existing or future legislation. Both aspects are covered by this Guide.

General guidelines to establish good occupational health and safety systems in the workplace are given in the joint Australasian Standard AS/NZS 4804:1997 *Occupational health and safety management systems - General guidelines on principles, systems and supporting techniques*. Conforming to this Standard requires an organisation not only to take account of legal requirements under the 1992 Act, but also it has a programme of "continual improvement". Since there are differences in the Australian and New Zealand legislative and regulatory frameworks, a new standard has been published as a New Zealand Standard only: NZS 4801 (Int): 1999 *Occupational health and safety management systems - Specification with guidance for use*. This Standard provides an audit tool so organisations can have their system certified against a recognised standard or it may be used as an internal check on current practices and procedures. Workplace-risk management is discussed in more detail in Chapter 8.

There are a number of international standards and guides. The joint Australasian standard has its counterpart in the Canadian Standards Association's publication *Risk Management: Guideline for Decision-Makers* CAN/CSA-Q850:1997. The British Standard BS 8800 gives a guide to occupational health and safety-management systems. It builds on the earlier standards such as BS 5750:1987 on the principles of quality assurance and BS 7750:1992 *Specification for Environmental Management Systems*. These have their international counterparts in AS/NZS ISO 9001 on quality and AS/NZS ISO 14001 on environmental management, respectively. A further international standard, ISO 14971, deals with the application of risk analysis in the management of medical devices.

A number of bodies in the United States produce a significant amount of information and guidance in fields relating to risk. In particular, the US Environmental Protection Agency (USEPA) is often cited in works relating to environmental effects and associated health risks. Unfortunately, the American use of a number of terms such as "risk assessment" differs from that in the joint Australasian Standard and many other international standards, and confusion can arise if US-based procedures are employed, which invariably adopt American terminology that is different from local usage. This book follows AS/NZS 4360:1999 in its use of language.

Overview of AS/NZS 4360

An overview of the main elements of the risk-management process, as set out in AS/NZS 4360, is shown in Figure 2.3, and elaborated in Figure 2.4 .

From Figures 2.3 and 2.4, it can be seen that the risk-management process consists of establishing the context; identifying, analysing, evaluating and treating the risks; monitoring and reviewing the performance of the management system and changes that may affect it. The Standard notes that it is vital to communicate and consult with both internal and external stakeholders, as appropriate at each stage, as well as concerning the process as a whole. This process can be applied at many levels in an organisation, to its strategy as well as its operations, and can be tailored in detail to a given organisational scale. It may be applied to specific projects or in the management of recognised specific areas of risk.

1 *Establishing the context*. The initial step is establishing the strategic context, the relationship between the organisation and its environment, through identifying the organisation's strengths and weaknesses, opportunities and threats. This context includes all aspects of the organisation's functions, not merely its engineering or technological aspects. At this stage, the vari-

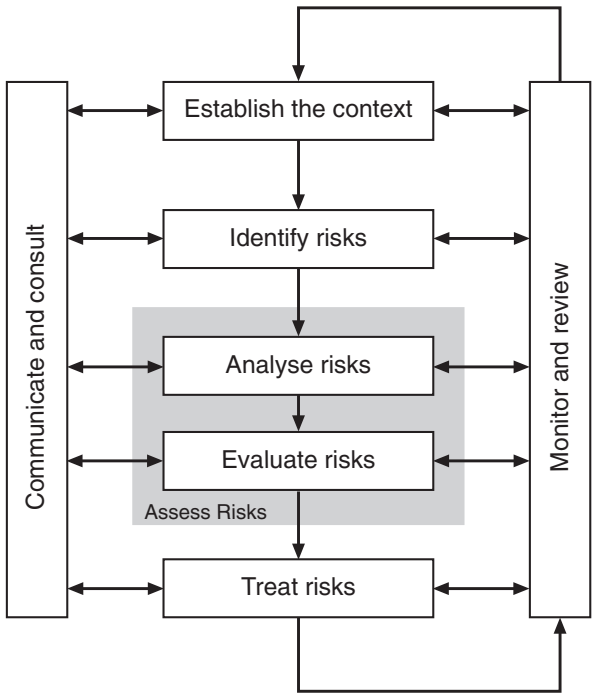


Figure 2.3: Risk-management overview (AS/NZS 4360: 1999)

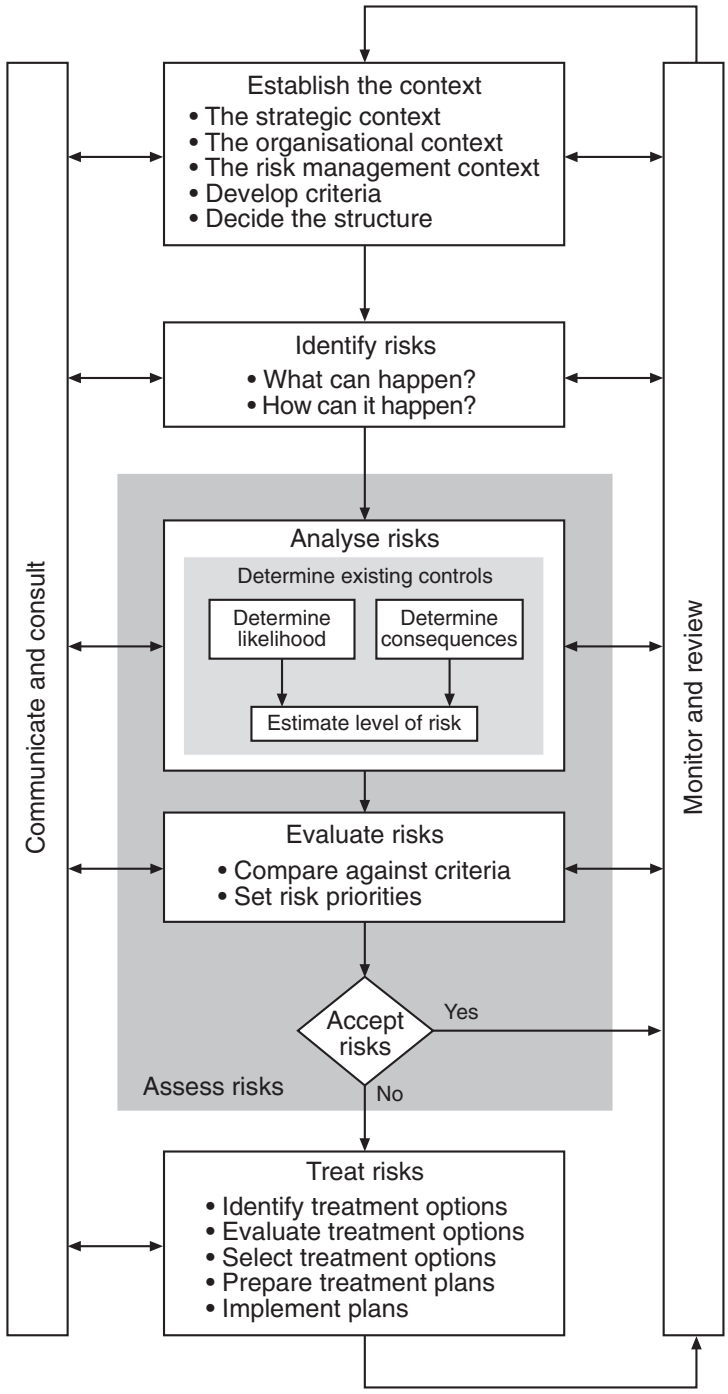


Figure 2.4: Risk-management process (AS/NZS 4360: 1999)

ous interested and affected parties or "*stakeholders*", both internal and external to the organisation, would be identified and policies to communicate with them developed. Successful communication demands that each participant understands what the other is saying and there is goodwill to achieve an agreed outcome. The organisational context should be established, to understand the organisation's mode of operation and capabilities, as well as its strategic goals. Failure to meet the specific objects of the proposed activity or project should be one of the set of risks to be managed. Organisational policy will define the criteria for setting risk targets, whether a given risk is acceptable or not, and forms the basis of risk-treatment options. Finally, the activity or project would be divided into a set of elements to provide a logical framework for later identification and analysis of risks.

The scope of a risk study can be visualised in terms of an input/output diagram, as shown in Figure. 2.5. The inputs are the range of hazards to be defined, while the outputs are the types of risks that are of interest.

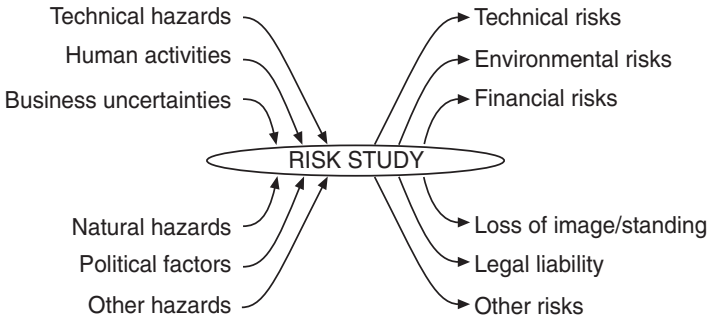


Figure. 2.5: Establishing the scope
(after Bermingham 1999, pers. comm., with modification)

2 *Risk identification, analysis and evaluation*. These aspects are considered in greater detail in Chapters 4 to 6. It is important to adopt a well-structured systematic process for the identification of risks, since an unidentified potential risk is excluded from any analysis. The survey should include all risks, whether under the control of the organisation or not. The aim is to generate a list of events that might affect each part of the activity or project, their possible causes and scenarios.

Once the set of risks has been identified, the next stage is to rank the risks, to determine those that can be tolerated and those that must be treated. The analyses would consider the likelihood and consequences of an event should it happen, in the context of existing controls or mitigating measures. Sources of information for this work include past records and expe-

rience, engineering or other models, expert judgments and failure databanks. The analysis may be undertaken to various degrees of refinement, depending upon the risk data available and the significance of the identified risk.

Such analyses may thus range from simple qualitative assessments to detailed quantitative estimates based on engineering-failure models. Since some of the estimates made in such quantitative analyses are imprecise, a sensitivity analysis should be carried out to test the effects of changes of assumptions and data. Finally, the risks are evaluated in terms of the earlier-set criteria or targets.

In analysing risk, it is useful to bring together people with differing backgrounds at this stage, each viewing the world in differing ways. Our life and professional experiences shape the way we think. In many cases, it is person-to-person communication, person-to-machine and person-to-environment interaction, which provide the commonest sources of risk. Organisational hierarchies can attenuate knowledge of the actual operating conditions, with higher levels of the organisation being unaware of risks, while organisational change can cause a loss of corporate/institutional memory.

A good example of a lack of knowledge about the risks of operation as decision-makers became progressively removed from day-to-day operations is provided by the Presidential Commission established to inquire into the cause of the space-shuttle *Challenger* disaster in 1986. (The detailed background to the failure is given in Case Study 2.2.) The Commission concluded that the decision to launch was flawed because those who made the decisions were unaware of the history of problems with unreliable seals in the booster rocket, as well as the contractor's advice not to launch at low ambient temperatures. Even the contractor's technical managers appeared to lack a full understanding of the likelihood of failure, which was known only at the technician level amongst those assembling the booster rocket.

The multilevel management structure, in which the highest levels were removed from the workface, is illustrated in Figure. 2.6. The cause of this lack of knowledge of management, both at Levels I and II, about the risks of the operation was found to be the tenuous management structures.

The likelihood of risks can be conveniently plotted on a graph with logarithmic axes, as shown in Figure 2.7, which is often called the *risk profile*. This representation greatly simplifies the visualisation of relative risks, and the setting of boundaries between intolerable ones and those that might be considered negligible. There is a broad band where risks fall in a region that risks might be considered tolerable for the time being, but where the organisation is obliged to reduce these to "as low as reasonably possible",

Case Study 2.2 Failure of Risk Communication: the *Challenger* Disaster

(a) Summary of Events

The cause of the tragic *Challenger* accident on 28 January 1986, when a space-shuttle rocket booster exploded after lift-off, was systematically traced to a faulty design of an O-ring seal. The flight began in the late morning (11.38 am) and ended 73 seconds later in an explosive burn of hydrogen and oxygen propellants that destroyed the external fuel tank and exposed the space-shuttle to severe aerodynamic forces that caused complete structural break-up. All seven crew members perished.

The explosion was found to have been caused by hot combustion gases that escaped from a booster via a failed field-joint seal. The joint design included two O-rings that did not function correctly at launch due to the low ambient temperature that prevented them from responding correctly to the rising pressure after ignition and movement (rotation) within the joint.

Engineers had held concerns regarding the behaviour of the seals at low temperatures for a number of years prior to the tragedy occurring and low temperatures were forecast for the morning of the launch. As noted by Pinkus et al.[3], analysis of the records showed that of the previous 23 launches in which the field-joints had been examined following booster recovery and where data was held, seven showed damage to the O-ring seals. This damage had only occurred at ambient temperatures below 24˚C and it occurred in all cases where the temperature was below 18˚C. The lowest temperature recorded was 12˚C. However, various factors, including the management structure of the project, and ultimately time pressures to maintain the space-shuttle programme, created a situation where launch proceeded despite technical advice to the contrary and at an ambient temperature near to freezing (where seal damage was very likely to occur).

(b) Technical and Managerial Reasons for the Failure

(Information from the Presidential Commission report, Bermingham, 1999, *pers. comm.*)

Technical Details

The technical cause of the accident was traced to hot gas escaping (known as *blow-by*) following the failure of the O-ring pressure seal in a joint of the casing of the booster. The failure was due to a faulty design, unacceptably sensitive to a number of factors including, the effects of temperature, physical dimensions, the character of the seal materials, as well as the reaction of the joint to dynamic loading. The Shuttle's solid rocket boosters were made up of several sub-assemblies; the nose cone, solid rocket motor, and the nozzle assembly. Marshall Space Flight Center was responsible for the solid rocket boosters, while Morton Thiokol was the contractor for the solid rocket motors. The boosters are one of a set of '*elements*' that make up the complete craft.

Each solid rocket motor case is made up of 11 individual weld-free thick-walled steel sections about 3.5 metres in diameter joined together. When assembled they form a casing tube 35 metres long. After partial assembly the propellent is poured (cast) within the casing. Within each joint two O-ring seals, protected by high-temperature putty, act to contain the pressure caused during flight by the rapidly burning solid propellent.

The Decision to Launch (refer Figure 2.6)

Although as stated above, the technical cause of the Challenger's explosion was the result of a failed O-ring seal, the Presidential Commission tasked with investigating the disaster found that the underlying cause *was rooted in organisational failures and poor communication.* Prior to the launch of this flight, the procedures of the Flight Readiness Reviews (FRR) were carried out in accordance with normal procedures. However, concerns of Level III NASA personnel, and element contractors, regarding the joint seals of the Solid Rocket Motors were not adequately communicated to the NASA Level I and II management responsible for the launch. The Level I and Level II managers were unaware that the O-rings had been designated a "*Criticality 1*" feature – a term denoting a failure point, without back-

up, that could cause a loss of life or vehicle if the component fails. This component had previously been designated "*Criticality 1R*" – the R implying redundancy. The R was removed when it became understood that the secondary O-ring was unlikely to seal if the primary O-ring failed.

The Level I and Level II managers were also unaware that since July 1985 a launch constraint had been imposed and then for six consecutive flights waived. The crucial factor seems to have been that *neither the management of Thiokol nor the Marshall Level III manager believed that the O-ring blow-by and erosion risk was critical*. The testimony and contemporary correspondence show that Level III believed there was ample margin to fly with the extent of O-ring erosion that was being experienced, provided the leak check was performed at an increased pressure. The fact that the increased test pressure was a contributor to the increased failure rate in service seems not to have been recognised. *What is clear is that the NASA Level III managers, and Thiokol management, had no such understanding, or at least had a different perspective of the failure mechanism to that held by Thiokol's engineers*.

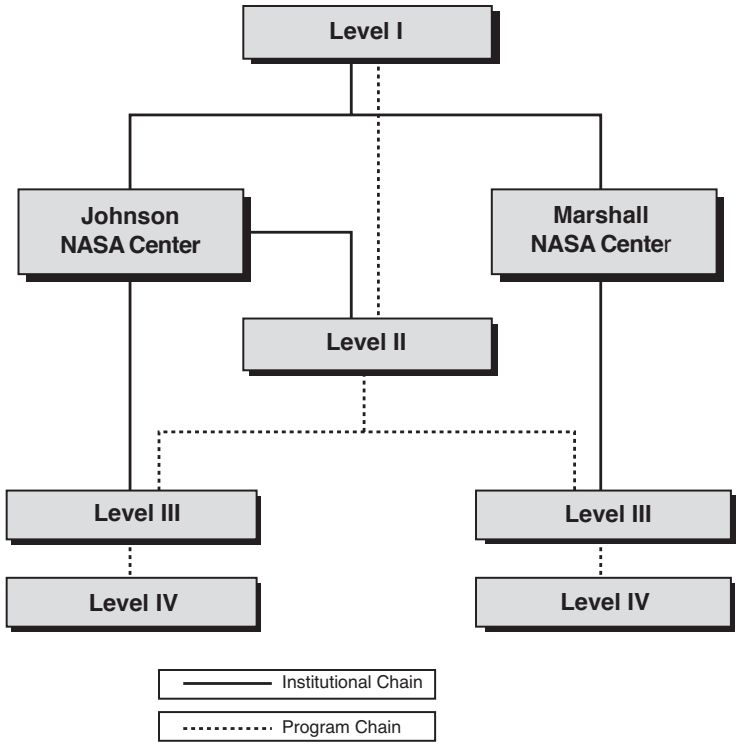
The Mission Management Team (MMT) postponed the launch scheduled for 27 January due to high crosswinds. The MMT met again at 2.00 pm on that day and concerns were raised about the effect of the forecast low temperatures on such facilities as drains, eye wash and shower water, and fire suppression systems, but not about the O-rings. When the situation was relayed to the engineers at Morton Thiokol they were adamant about their concerns over the low temperature – "….. *way below our database and we were way below what we qualified for* …..". They contacted Morton Thiokol's liaison officer at the Kennedy Space Center, expressed their concern, and requested more forecast temperature data. He recognised the significance of the concerns and ensured that a teleconference was set up. This was in turn followed by a second.

At the second teleconference Morton Thiokol engineers presented the history of O-ring erosion and blow-by. Their recommendation was not to launch until the O-ring temperature reached 53˚F (12˚ C). A long, detailed, and reportedly not acrimonious discussion followed. Thiokol's Vice President of Engineering was asked for a recommendation and he replied that he could not recommend launch. The Deputy Director, Science and Engineering at Marshall, was reported to have said he was "appalled" at the recommendation not to launch. The Manager SRB (Solid Rocket Booster) Project at Marshall was said to have asked, "*My God, Thiokol, when do you want me to launch, next April?*". Under this pressure, Thiokol management asked for a recess to consider their recommendation further and a Thiokol management-level discussion took place. One of the managers is said to have remarked that he "*took off his engineering hat and put on his management hat*". The Thiokol managers seem to have concluded that, although blow-by and erosion was to be expected, there was no evidence to predict joint failure. In the lack of such evidence Thiokol withdrew their recommendation not to launch. As one of the Thiokol engineers described it, "*This was a meeting where the determination was to launch, and it was up to us to prove beyond a shadow of a doubt that it was not safe to do so. This is in total reverse to what the position usually is in a pre-flight conversation or a flight readiness review*".

The launch subsequently took place, with fatal results.

Conclusion

The Presidential Commission concluded that the communication failings that contributed to the disaster were caused by *the complex and ill-conceived management structure in place at the time* (Figure 2.6). Although a complex programme such as the shuttle will inevitably involve a complex organisation to manage it, the actual set-up was made unnecessarily complex in response to the lobbying of individual states involved in the US space programme for their "share of the action". The Commission found that the management structure led to the project managers of the various elements of the Shuttle programme feeling more accountable to their centre management (Institutional Chain in Figure 2.6) than to the Shuttle programme organisation (Program Chain in Figure 2.6). Funding, work package definition and vital programme information frequently bypassed the Program Manager (Level II).



Level I
The associate administrator for Space Flight Oversees budgets for Johnson, Marshall and Kennedy NASA centers. Responsible for policy, budgetary and top level technical matters for Shuttle program.

Level II
Manager, National Space Transportation Program. Responsible for overall supervision of Shuttle program. Provides technical oversight on behalf of Level I.

Level III
Program managers for Orbiter, Solid Rocket Booster, External Tank and Space Shuttle Main Engine. Responsible for development, testing and delivery of hardware to launch site.

Level IV
Contractors for Shuttle elements. Responsible for design and production of hardware.

(Adapted from Presidential Commission report, Bermingham 1999, pers. comm.)

Figure 2.6: Management structure for the Shuttle program.

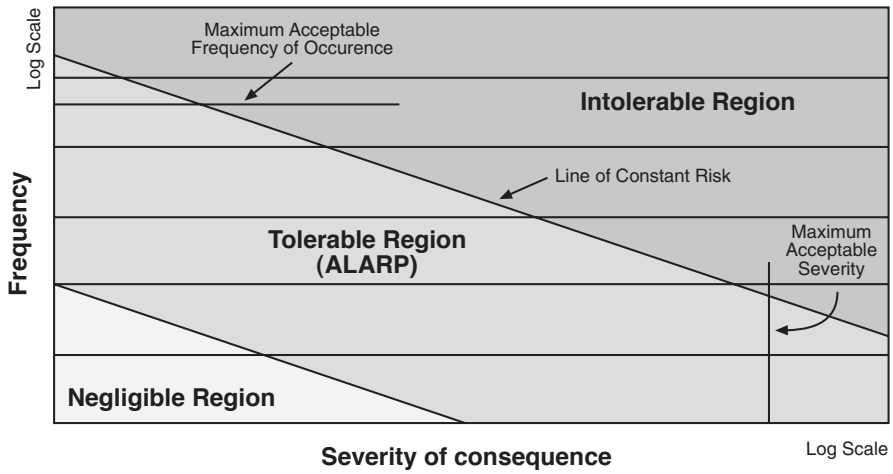


Figure 2.7: The tolerability of risk

the so-called ALARP region. The risk profile also shows that the greater the chance of something happening, the less severe is the likely consequence. This observation leads to two other limits: failures that have a maximum acceptable frequency of occurrence (because they may foreshadow something worse or simply soak up resources), but also there is a maximum acceptable severity irrespective of the remoteness of the risk.

For both a risk manager dealing with risk in general terms, or a project engineer investigating specific risks in detail, this process greatly simplifies understanding of the significance of risks. The various boundaries and limits are shown qualitatively because their values reflect society's concerns and individual philosophies. Some of the various suggestions for setting these limits are considered further in Chapter 6, as well as the background to the development of the risk profile.

Normally, the frequency or likelihood is measured in terms of the number of events over a stated period. In some cases of rare engineering failure, this time period can be very long for a single event to be witnessed at a particular site (in hundreds or thousands of years). The remoteness of such failures can be obtained by aggregating experience over a number of sites.

The scale of severity of consequence may relate to harm to persons, facilities, the environment or even business reputation. One simple scale is illustrated in Table 2.1

A significant problem faced by management during the evaluation of risks is the selection of the appropriate next step. As noted before, some risks will be clearly unacceptable to an organisation or society, whilst others

Table 2.1: A simple severity scale

Event	Code	Level	Value/Harm
Major business collapse	A	V	100 000
Major loss of business	B	IV	10 000
Major disruption, customer dissatisfaction	C	III	1000
Disruption to output, visible to public	D	II	100
Minor disruption to output, not visible to public	E	I	10
Minor incident no direct cost	F	0	1

Notes: The scale of cost or harm may be in monetary terms or represent the magnitude of the effect.
See Case Study 2.3 for the use of such a scale.

will be so small as to be of no concern. Those that fall in between, in the so-called ALARP region, will require further analysis and consideration. Even the sum of individual tolerable risks after treatment may be intolerable. An organisation having a very low risk of failure to an individual

Case Study 2.3 Manufacturing Plant Fire Risk
(Bermingham, 1999, *pers. comm.*; courtesy, New Zealand Pharmaceuticals Ltd)

The pharmaceuticals company was considering the fire-protection arrangements at their plant in Palmerston North. A risk-based review was seen as offering the best way of identifying the optimum allocation of resources.

For analysis purposes, the manufacturing site was split into areas (fire cells) and an inspection of each was carried out by a qualified fire engineer. The likelihood of a fire starting in each area was judged and the various fire protection options for each cell or area identified. The likelihood assessment was based upon experience as well as published fire data. The company's Board was separately asked to assess the consequence on their business should each identified element of the manufacturing plant be either damaged or destroyed by fire. This assessment was made against a previously defined consequence scale similar to Table 2.1.

Despite its relative simplicity and low cost, the study allowed the company to focus their intended fire protection expenditure in terms of the protection afforded to the business. This is as opposed to a more standard and less systematic assessment of immediate effect on each asset.

facility or asset may have a frequent incidence of failures if the number of facilities or assets is large. The organisation might therefore find itself defending its operations frequently, at a significant distraction and cost.

3 *Risk treatment*. Once the range of unacceptable risks has been identified through the foregoing steps, the various options for treating the remainder are considered. These include reducing the likelihood of the risk, or reducing its consequence, or transferring it in full or part. In engineering work, the opportunities for simple risk transference are limited. (One example is that it is becoming increasingly difficult to find landfill sites because of strong public opposition to locating sites "in my back yard".) However, the risk may often be avoided altogether by choosing a more prudent solution to the original problem.

Whenever there are a number of risk-treatment options, the alternatives

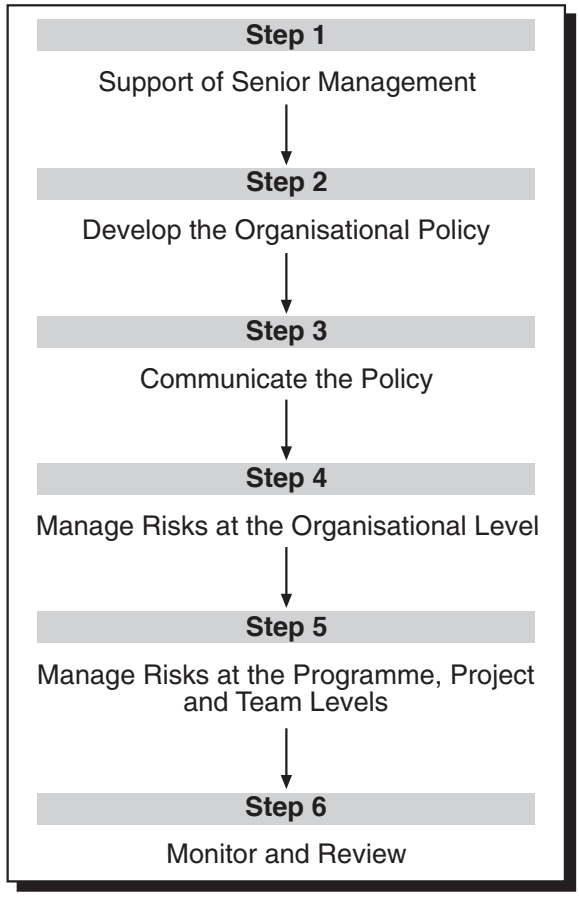


Figure 2.8: Steps in developing and implementing a risk-management programme (AS/NZS 4360:1999)

are assessed on the basis of the extent of risk reduction and the additional benefits or opportunities created, if any. Responsibility for the implementation of the selected option should be borne be those best able to control the risk. Should there remain a residual risk after treatment, a decision has to be made whether to accept this risk or consider further risk-reduction measures. Since there is societal expectation of ever-increasing standards of performance and safety, it is most likely that such risk reduction will be an ongoing process of stepwise improvement.

4 *Monitoring and review*. Few risks remain static. It is necessary to monitor the residual risks and the effectiveness of the control measures, as well as the management system set up to supervise the implementation of them. Risks can change, and control measures can become degraded or antiquated with time. Ongoing review is essential to ensure that the risk-management plan remains relevant.

The Australian/New Zealand Standard suggests a six-step programme to implement a risk-management programme, as set out in Figure. 2.8.

5 *Communication and consultation*. The Australian/New Zealand Standard emphasises the need for communication and consultation at all steps in the risk-management process, with a plan in place at the earliest possible stage in the process. Perceptions of risks can vary according to differences in concepts and desires among the various stakeholders. The Standard recommends that both perceptions of risks and perceptions of benefits be identified and documented, so that the underlying reasons for them is understood and addressed.

Ongoing Risk Management

The Australian/New Zealand Standard emphasises that *risk management is an ongoing aspect of an organisation's operations*. Appropriate risk management is concerned with preventing future loss. Lack of such management can lead to sudden and very public failures, with attendant loss of goodwill and costs to the organisation, as recent major incidents in both Australia and New Zealand have shown.

Risk management is not an established discipline. It requires education and training in techniques, some of which are outlined in the remainder of this book.

Risk management is exercised at all levels in an organisation. All managers inherently manage risk in their day-to-day work, so all are responsible at their own level. Every decision, at whatever level, whether made by committees or individuals, carry risk. *Consideration of risk needs to be a natural part of the decision-making process*. In time, it should become instinctive.

The world is changing. This has always been so, but the pace has quickened and now is more perceptible. Even when no specific decisions have been made, the organisation's risk profile will have changed with time: some risks will fade away, while others will develop in significance. *The management of risks needs to be planned, proactive and permanent*, whether there exists a specific committee with particular responsibilities or these are incorporated in other management groupings.

Risk Analysis as an Engineering Management Tool

The following generic example in Case Study 2.4 demonstrates ways in which a risk-management programme at the working level can reduce future losses within an organisation.

As noted by Peet and Ryan[4] in their description of the risk-management system for a rail network, from a business perspective, one of the main purposes of integrated risk management is that it provides a framework for making difficult decisions. Such a management process provides opportunities for improvement and for minimising potential failures. Rail networks are subject to external threats, such as those from storm and earthquake, as well as more controllable internal failures of people, systems and equipment.

Case Study 2.4 A Risk Management System for a Rail Network

Peet and Ryan[4] cite three case studies of risk assessment that formed part of developing the overall risk management of the network for Tranz Rail.

1. Collision between trains. Both the signalling system and the people involved in the operation of the railway are key parts of the safety systems that prevent collisions between trains. The commonest approach to controlling train movements is to use coloured-light signals that instruct the train driver: red to stop, yellow for caution and green to proceed. On lower-trafficked lines, no colour signals are used, as authority to occupy a section of the line is given by warrants transmitted by radio or line phone by a train controller. A verification procedure is used to control the risks of wrong communication. While automatic line systems have interlocking capability to prevent dual authority to enter a given section, they do not give the train controller any ability to change the signal-light setting. Centralised train-control systems have computer-aided checks to ensure that conflicting warrants to occupy lines are not given. The network is a complex interactive system involving drivers on opposite or overtaking trains, the train controller and physical systems such as signalling equipment and vigilance devices in locomotive cabs. Equipment may fail to operate correctly due to technical defects or be overridden, while the operating staff can fail due to fatigue, distraction, sickness or poor judgment.

To assess what was important and what was not, the risk assessment was broken down into two parts: the understanding of the risks of running trains, and determining which of those risks were affected by different signalling systems. This evaluation was undertaken by bringing together a group of people with a varied experience of the working of

the railway. The next stage was the development of a risk matrix of likelihood and consequence. In assessing the likelihood of events, it is often hard for experienced staff and lay persons alike to make a judgment and to compare different descriptions of remoteness. The greatest value of a risk matrix is to sort risks into broad bands of risk level. In this case, the matrix approach was able to illustrate the relative significance of the risks; but, due to the coarseness of the method, it was not useful for understanding any differences in signalling systems. However, the method was entirely adequate as a scoping study to compare drivers' risks as part of a wider study of risks borne by all employees.

A more detailed study required modelling the fault and failure-propagation process with techniques such as fault-tree analysis. Such methods are outlined in Chapter 5. These methods involve determining the structure of incidents and looking how the various components interrelate and interact, whether human, systemic or hardware-related. A fault tree can be developed at various levels of detail, enabling the quality of the safety procedures to be ascertained. Historic data on failure rates of components and experience of human reliability can then used with the fault-propagation model to estimate the likely frequency of the particular event of concern, in this case, the chance of a collision of two trains. The answer could be checked by "benchmarking" intermediate failure events with actual known rates from incident databases.

2. Transport of hazardous goods. In this case, a study was undertaken to gain a general understanding of those parts of the network that handles hazardous materials and the types and quantities of goods transported. The study was to describe the main hazards presented in this traffic, and thus make preliminary recommendations for its risk management. The work was broken down into five parts: classifying the types of goods handled; identifying accident scenarios; defining the range of impacts from possible incidents; assessing the pathways and consequences of these incidents; and finally, assessing the relative risk level. The focus was on leak or loss of containment. Generic kinds of accidents were identified, such as derailment or collision, and then the failure modes by which these events might take place, like track or point failure. The failure modes were further broken down to find the prime causes. Three different scales were developed, with each scale assigned a range from 1 to 6. The first scale was one of likely frequency based on experience; the second was a scale of consequence to people, the environment and property and the third assessed the likely magnitude of cumulative effects for accidents that happened repetitively. The total risk or outcome was assessed by multiplying the likelihood and consequence scores and adding the cumulative effect score. The sensitivity of the result was tested by using different weightings on the input scores.

The results were used to assign priority for follow-up action. The proposed measures included a review of incident-reporting systems to enhance the quality of information; refresher training for operating staff in handling and administration of hazardous goods; and a safety audit of the handling of liquefied petroleum gas (LPG) from loading to empty return of railtanks to customers. The risk-management strategy focussed on ensuring compliance with all aspects of approved procedures.

3. Single-manning risks. At the time when electric locomotives were being introduced on the North Island Main Trunk (NIMT) between Palmerston North and Hamilton in the mid-1980's, it was decided to assess the risk of changing from two-man crews to single manning. The accidents to a driver include collisions, overturning and derail-

ments. Not only are there risks while driving but there are external risks in breakdowns or emergencies, particularly as a significant number of services were run at night. For each kind of accident, a fault tree was developed that incorporated mechanical, procedural and human-failure elements. Data were generated from experience, estimation, sampling, surveys and expert opinion, including industrial psychologists. Rough relative comparisons could be made with other industries by comparing fatal accident rates (FAR), as described in Chapter 6. The results suggested that the risk level to train drivers was lower than many occupational groups in the company and in other industries. It was considered that the risk assessment was a significant factor in the company being able to negotiate an industrial agreement incorporating single manning of locomotives.

Tranz Rail has used formal risk-assessment techniques for over a decade to develop a culture of risk awareness within the company. Experience gained from the various projects have included the following:

- Pulling together small groups of respected staff and specialist experts under the leadership of a risk-assessment manager has been a powerful means of raising this awareness.
- The scoping phase of a risk assessment is often enough to rank and prioritise the allocation of resources efficiently for alternative courses of action within given risk targets.
- Quantification of issues reduces emotion from discussions and can be a powerful decision-making aid for management, especially whenever the results are combined with the cost consequences of various actions.
- Quantified risk assessments show the various contributors to the risk and their interaction. While sensitivity studies can be done on some of the more critical elements to understand better the range of likely outcomes, the use of extreme values for component reliability, in an attempt to show the robustness of the model, leads to unnecessarily lengthy explanations to gain a balanced perspective.
- Development of failure-propagation models, such as fault trees, requires considerable work to ensure that all possible sources of risk are accounted for. Data for the fault trees require considerable research and are often not in the right form or lack consistency or completeness.
- It is likely that at some stage, given enough time, a significant accident will occur that is likely to draw media attention. Communicating, understanding and use of the results of risk assessments by third parties remain a problem. Risk-assessment techniques alone are no substitute for sound management practice involving quality assurance of the existing systems needed to control the operation.

Case Study 2.5 Setting of an Environmental Risk Bond
(Bermingham, 1999, *pers. comm.*; courtesy Watercare Services Ltd and the Auckland Regional Council)

The resource consents associated with the major upgrade of the Mangere wastewater treatment plant in Auckland were extensive. Amongst the conditions was the requirement that an environmental risk evaluation be undertaken to determine the level of bond to be lodged in favour of the Auckland Regional Council. The plant owners, Watercare Services Ltd, commissioned a risk evaluation both to aid environmental management of the plant and to establish the level of environmental risk in financial terms.

The particular requirements of the consent were:

a) Identification of the potential environmental risks arising from any failure to comply with the condition of consent;

b) Measurement of those risks;

c) The costs of remedying or mitigating any adverse environmental effects which may arise from such failure; and

d) Evaluation of an appropriate sum to adequately provide for such remediation of those risks.

Due to the size and complexity of the waste-treatment plant, the risk evaluation used a "bottom-up" approach. This ensured that all sources of risk were identified. A quantitative methodology was developed that allowed each fault sequence to be analysed and the associated costs of repair and environmental clean-up to be calculated. Due to the different nature of the risks during construction and operation, two separate but related studies were completed for these phases in the project.

The risk model was designed to allow differing conditions and assumptions to be considered and to enable a sensitivity analysis to be undertaken. The model outputs included the

- Repair and clean-up costs of the each incident,
- identification of the highest cost incidents,
- a quantification of the risks associated with each incident,
- the total environmental risk expressed in dollars per year.

Where the effects could compound, the associated events were combined to ensure that the calculated costs would include all remedial actions. In additional an allowance was included to cover other costs such as post-clean-up monitoring to confirm the effectiveness of remedial actions.

Watercare Services Ltd and the Regional Council initially started the exercise with significantly differing expectations of the appropriate level of a bond. However, the study enabled the two parties to quickly negotiate a bond value that was based upon the assessed environmental risk, as opposed to any previously perceived but unquantified level of risk.

References

1 Elms, D G (1998). "Overview - Prudence, principles and practice", in Elms D G (ed.) *Owning the Future: Integrated Risk Management in Practice,* CAE, University of Canterbury, Christchurch.

2 Hom, S and Ellis, M (1998). "A framework for managing risks associated with human-induced hazards", in Elms, D G (ed.) *Owing the Future. Integrated Risk Management in Practice*, CAE, University of Canterbury, Christchurch.

3 Pinkus, R L B, Shuman, L J, Hummon, N P and Wolfe, H (1997). *Engineering Ethics: Balancing Cost, Schedule and Risk*, Cambridge University Press, Cambridge.

4 Peet, W and Ryan, R (1998). "Risk management in a network operation: understanding complex systems", in Elms, D G (ed.) *Owing the Future. Integrated Risk Management in Practice*, CAE, University of Canterbury, Christchurch.

3 Nature of Risk

The Australian/New Zealand Risk Management Standard describes risk as the chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood. It may be an event, action or lack of action. Risk stems largely from uncertainty, as noted in Chapter 1. With financial risk, this uncertainty arises out of the unknowable future with the vagaries of the market and political change. With technical risk, this uncertainty relates to the probabilistic nature of certain failure sequences happening. The outcome is nearly always unwelcome or unwanted. Yet risk adds spice to life. The risk of things going wrong focuses our minds and spurs us to plan with greater forethought. On the other hand, things may go right, and we may benefit beyond our wildest dreams.

The above definition of risk is consistent with much current international practice and is broad enough to encompass most sectors and professions. There are many other variants. McNamee and Selim[1] give five different interpretations, and from the viewpoint of auditors decided on the following definition: risk is a concept used to express uncertainty about events and/or their outcomes that could have a material effect on the goals of the organisation.

According to Elms[2], risk has three aspects:

- the chance of the undesired event happening;
- the consequence should it do so, and
- the context in which the hazard might be realised.

There may be a chance of rain; the effect on us depends upon the standard of rainwear we have, and whether we are indoors or outside at the time it is raining. These three aspects govern the risk that we will get wet.

The Australian/New Zealand Standard recommends that the context in which a risk occurs should be established before the risks are identified and assessed. This consideration defines the framework within which the risk is to be managed and provides guidance for later more detailed risk-management studies, as noted in the previous Chapter. Too narrow a scope would result in hazards and their risks being overlooked, while one too wide or ill-defined would waste resources and detract from the core issues.

We differentiate between a hazard and its associated risk. A logging truck in the forest may be regarded as a hazard, since there is a possibility that the truck will overturn, spilling its load. A hazard is thus a situation that in particular

circumstances will lead to harm; it is the source of the risk. Before we can say anything about the risk of such an incident, we need to know something about the frequency (likely rate) of spills and the possible consequences (the harm and cost of damage) should they happen. Therefore, the risk of a particular hazard happening is a function of frequency and consequence, that is:

$$\text{risk} = \text{f (frequency, consequence)}_{\text{hazard}}$$

The lack of differentiation between a *hazard* and the *risk of its appearance* can lead to a wrong analysis. For example, corrosion of a pipe may be considered to be a hazard in the containment of a fluid, but the consequential appearance of a hole is not; this is the resultant event. Listing "hole-in-pipe" as a hazard would amount to double counting in this case.

Safety may be regarded as the inverse of risk; that is:

$$\text{safety} = 1/\text{(risk)}.$$

For this reason, a safety analysis is often concerned with determining the level of risk. A thing is safe if the risk is very small. Risk is never zero, neither is safety perfect. Safety measures reduce the risk by diminishing the likelihood of the hazard occurring and/or by interposing blocking or mitigating features to decrease the potential impact of the hazard. One needs to maintain a perspective. Excessive obsession with eliminating risk can make us nervous wrecks, and hinder development and opportunity. Like Hamlet: *do we rather bear those ills we have than fly to others that we know not of?*

The risk function is not a simple one. If the consequence is small, we often disregard the risk as being negligible. However, even if the frequency is very small, but the consequence very large, we often still consider the situation to pose a threat, or have a large risk. The debate on the safety of nuclear-powered warship visits to New Zealand ports focused on this issue, between those who pointed to the multiple safeguards and the extremely remote likelihood of a major incident happening and those who pointed to the far-reaching and disastrous consequences should it do so.

These definitions are given qualitatively, since we have no absolute standards of what is large or what is small; there is no standard yardstick against which to measure risk. We can, nevertheless, compare risk levels and rank hazards, and the development of suitable risk criteria is considered in Chapter 6.

Risks can take many forms. Some of these aspects that an engineer may face will now be examined.

Technical Risk

Technical risk is a major but not the sole component of engineering risk, which

includes other aspects such as commercial, organisational, political and social factors. It arises because of the likelihood of failure in the design, construction and operation of engineering systems and their components. All systems have some probability of failure, and a prime objective of engineers, when considering reliability, is the reduction in the incidence and impact of failures to levels that society appears to tolerate and businesses can bear.

The pace of modern industrial growth and technological development has brought problems which have given rise to debate and conflict on issues such as environmental degradation, resource and energy use, and the impact of toxic substances[3]. Developments are on a larger scale than hitherto, and economic considerations can often limit the full evaluation of possible effects of new work. The probability of fire in an industrial building increases with the size[4]. The complexity of projects, involving numerous teams and subcontractors, dilutes individual responsibility and increases the difficulty of monitoring by public inspectorates. There are many ways in which something can go wrong, but there is usually only one way that is right, and it is difficult to foresee all the potential problems before commencing a large project.

Problems and projects are becoming more complex, yet there are fewer technical staff to cope with them than formerly. Workers have been reduced in number to the minimum to look after and operate increasingly sophisticated equipment. Hard-pressed engineers may have difficulty in keeping abreast of the technical literature in their speciality, and their managers must be aware of developments over an even wider field. The chance of a mistake slipping though would seem to be greater. There is some evidence of this. A 1990 survey[5] of losses in the chemical and petroleum industries noted that the eight large losses recorded in the previous year were about 2.5 times the average of 87 other losses recorded over the years from 1960 to 1987, when measured in inflation-adjusted dollar values.

The basic technical risks of a project not only relate to the incorporation of new ideas and technology that have not been fully tried and tested for the particular application; they also hinge on the limitations of strength and resistance of embodied materials and structures to withstand the environmental and operating conditions, as well as the ability to cope with the unforeseen or unknowable deviations that may arise from time to time. A numerical estimate may be made regarding such risks. A structure built to a particular specification will have a calculable chance of collapse in an earthquake of given intensity. A high-pressure storage vessel for a flammable liquid will have a computable chance of failure in an engulfing fire for a given set of safety features and construction standards. Whether such technical risks of failure will be realised in practice depends upon various human factors: the accuracy of the specification, the quality of fabrication of the vessel and care in the installation, maintenance and operation of it thereafter. In this sense, the fundamental technical risk represents the

best that can be hoped for. The realised technical risk will always be somewhat greater because of these human factors.

A better understanding of engineering fundamentals, with enhanced and more precise design methods, have enabled engineers to work within ever-closer tolerances. Failures are then more likely to be sudden, with little warning. We need to know what margin of error we have, and have some quantitative "feel" for the remoteness of the embodied hazards. Methods for estimating technical risks are outlined in Chapter 5.

In some cases, investigation of past failures, such as those of box-girder bridges[6], provides an understanding of modes of failure. In general, the potential for grave consequences as a result from engineering mishaps is sufficiently great for it to be unacceptable to wait to gain information from disasters. The less commonly-observed failures are thus estimated from more frequently witnessed breakdowns and upsets *by synthesising possible pathways to failure*. Whenever there are a large number of triggering events, the uncertainty in the estimate of the ultimate outcome is relatively small: whereas, whenever a large number of mitigating or protective features are introduced to reduce the incidence of a hazard, the calculation of the outcome is relatively uncertain (although it may be remote)[7]. *By the nature of things, we can only be very certain about events when they happen frequently.*

Computer-related Risks

Computer-related risks produce particular kinds of technical risk. Increasingly, and in some cases exclusively, engineers rely on computer software to undertake their design calculations as well as to control systems. The power of these design tools can easily seduce practitioners to make estimates beyond the range of variables and conditions for which the software has been derived. Moreover, such embedded limitations may not be explicit or clear in the documentation, even if still available to the engineer. The numerical calculations may be lengthy, and impracticable to confirm by alternative hand calculations. It is often difficult for an inexperienced engineer to know whether an obtained answer is realistic or not. In the case of new technology or the analysis of infrequent events, there may not be corporate experience (or institutional memory) either. Some common sources of error in the computer-aided design of process plants is given by the Institution of Chemical Engineers in their 1987 guide to the responsibility of engineers for their computer-based decisions.

Intelligent and computer-aided systems for control and monitoring are almost universal in engineered plant and facilities. Such systems may involve complex network arrangements and remote sensing of equipment status, with the minimum opportunity for manual intervention. Errors can arise if the software engineer does not fully understand the plant or process, or the practising engi-

neer is unfamiliar with the program and its diagnostic tools because of their complexity. In-house programs, being familiar to their originators, can often suffer from inadequate documentation for others to follow, with attendant risk of misinterpretation of the designer's intent.

Kletz[8] relates one amusing incident involving computer control: one night, at the end of summer time, a process operator put back the clock on the plant's computer one hour. The computer then shut down the plant for an hour until the clock caught up with the program!

Even highly-developed, safety-critical software can fail. A board of inquiry into the loss of an early Arian 5 rocket, which was traced to a simple software error, ruled that all software should be assumed to be faulty unless proven otherwise (*New Scientist*, 28 July 1996).

Even elementary errors can creep in. A review board, in the release of its findings into the break-up of the first interplanetary weather satellite in the Martian atmosphere, attributed the loss to a "systems-engineering failure" (The Christchurch *Press*, 2 October 1999). Apparently, in making a key change to the spacecraft's trajectory, one team used Imperial measurement units and another the SI system!

System and Management-related Risks

Often in inquiries set up to determine the technical reason for an accident, the underlying cause of the incident is some management or system breakdown.

- On an offshore gas platform in the **North Sea (Piper Alpha)**, the failure of one shift to inform the following shift that some maintenance was being done led to a sequence of failures causing a gas explosion which ultimately resulted in the complete destruction of the platform itself.
- At **Seaview near Wellington**, a weakness in engineering infrastructure resulted in a lack of understanding of the hazards of heating together two immiscible liquids in an oil re-refining process. Oil and water separated in a vessel after a shut-down, resulting in a steam explosion which caused a fire that gutted the whole works.
- The failure of a viewing platform at **Cave Creek on the West Coast** was as much a management-system failure as a serious deficiency in the engineering design and construction procedures.

Management-related risks are seldom obvious to managers. Over the last decade, there have been significant changes in management structure, with smaller in-house engineering teams. No longer are there large Government departments within which there is retained significant engineering experience built up over a long period. The changes have brought about a corporate (or institu-

tional) memory loss that has not been entirely replaced by external consulting services or through computerised records. *Only people have active memories, and when they move on or out, they take this knowledge and their experience with them.*

However, the "memory" of an organisation may be improved, as Kletz[9] suggests, by using formal information systems to remind operating staff of potential hazards in their work and to record the past history of equipment operability for the benefit of maintenance crews. *To warn us of problems, the loss of corporate/institutional memory means that we must now depend more heavily on adequate formal records and the reliability of automatic monitoring and surveillance systems.* There is less direct human insight. Yet, at the same time, stricter planning and safety controls insist on minimal risk to the environment and to people.

Moreover, our systems have become more complex and interdependent. Economies of scale have seen huge increases in production rates at single facilities. The growth of dairy factories from many small farmers' co-operative enterprises to a few large milk-processing plants is an example of this trend. Milk is transported (at some risk) over many kilometres by tanker-trailers by road to these huge plants in which several megalitres of milk are converted daily into a range of products involving advanced process technology. Milk-powder plants, for instance, were formerly operated at relatively low temperatures with single-stage dryers. Today, much higher inlet-air temperatures are used, fine powder is recirculated to get larger particles, and the drying is undertaken in two or three stages with the partially dried powder being conveyed in warm air. The risk of a serious dust explosion is much enhanced, requiring greater skill in the design and operation of the plant than before to maintain safe working conditions.

Environmental and Ecological Risk

Environmental risk refers to threats to the world surrounding a particular activity or facility. *Ecological risk* refers to threats to particular ecosystems. When developments were small, ill effects were only local in impact. There was always an escape to an unsullied environment. *Indeed, the belching chimney and the waste tip were once viewed as a sign of industrial progress!* Today, our activities are on such a scale that ill effects cross national boundaries:

- the fall-out from a fractured nuclear power station in the Ukraine rained over much of Europe;
- the gas-borne pollutants from Britain's coal-fired power stations land in Scandinavia;
- the smoke from forest fires in Indonesia spread throughout South-East Asia.

Indeed, there are now substantial worries that increasing worldwide industrial activity may even be causing significant climatic changes with far-reaching consequences for life itself on earth.

Although the effects of fires and large-scale accidents (such as toxic releases) can be evaluated, it is more difficult to assess the impact of frequent but small-scale events that ultimately may do more damage to the environment. The slow dribble may do more long-term harm than a massive single leak. Monitoring, when the problem is evident, may be too late.

Since environmental impacts may be wide-ranging and long-lasting, some authorities[10] prefer to speak of ecological risk in which the effects on whole ecosystems are considered, rather than the impacts on aspects of the built environment or particular parts of the natural world that are prized by people. Unresolved in many cases is the precise thing to be protected; and even when that is defined, it is not easy to find a useful means of measuring or monitoring the effects.

Modern concepts of inherently safe plants and cleaner processes imply that the environmental risk is much diminished if these principles are embodied in actual facilities. *Loss prevention and waste management require corporate commitment, but this policy can bring rewards in greater profitability and easier acceptance of development plans by consent authorities.*

Environmental risk is sometimes used in the narrower sense of the risks to management of legal sanctions from failure to meet and/or contraventions of statutory requirements under environmental legislation such as the Resource Management Act 1991.

Commercial and Business Risks

Engineering services meet human needs, real or perceived. In many cases, and increasingly so, these services are undertaken within a commercial framework. That a project is a technical success is in itself no guarantee that it will not be a commercial failure. Some significant innovative processes, such as the Taranaki gas-to-gasoline plant and the Glenbrook ironsands-reduction mill are highly successful in the technical sense, but their operations have been overshadowed by changes in the commercial climate since the projects were conceived in the "*Think Big*" era of the late 1970s and early 1980s.

Multipurpose facilities can respond more easily than single-stream production units to changing market requirements. However, the former often sacrifice efficiency for flexibility, with lower business risks, and the capital costs will be higher than plant designed for one product.

Most business risks are entered into for financial gain. The provision of venture finance is an example of a high-risk, high-gain activity. Gambling is an-

other kind of high-risk venture, with the prospect of a substantial but remote gain from the investment. In this sense, financial risks differ from technical risks that are sought to be eliminated, reduced or mitigated.

Risk financing refers to the business of setting aside funds to cover risks. Large companies often undertake a high degree of self-financing, but smaller firms normally resort to insurers for this purpose.

Classification of Risks

The original 1983 book, *Engineering Risk,* of the IPENZ President's Task Committee commented that it is difficult to classify risks suitable for shaping or guiding policy. Some discussion points are given by Lowrance[11] in his seminal book, "*Of Acceptable Risk*", in which he provides an array of aspects which govern peoples' attitudes to risk. A modified form of Lowrance's listing is set out in Table 3.1.

Table 3.1: Considerations affecting safety judgements (after Lowrance [11], modified)

More tolerated	Less tolerated
Risk assumed voluntarily	Risk imposed involuntarily
Risk assumed at work	Risk caused by work
Effect delayed	Effect immediate
Effect temporary and reversible	Effect long-lasting and irreversible
Effect known and minor	Effect uncertain and life-threatening
Exposure deemed necessary	Exposure unnecessary
Common hazard	Dread uncommon hazard
Affects all people	Affects sensitive people
Likely to be used as intended	Likely to be misused

The table highlights one important aspect of the way in which we assess risk. "*We are loath to let others do unto us what we happily do to ourselves*." (Chauncey Starr). Whenever the risk is apparently our own choice, then we are prepared to undertake hazardous activities. We climb mountains, ski down slopes, use hand-tools without proper safeguards, smoke cigarettes, eat the vegetables and fruit that we ourselves have sprayed; but we do object to the cellphone tower in our neighbourhood or the coal burners at the college next door.

This difference of regard has led many observers to comment that risks involuntarily thrust upon us should be treated as being more serious than those of our

own choosing. This line of reasoning can support the view that pursuing one's trade will almost invariably bring a peculiar set of risks and, moreover, that such risks may be allowably greater than those outside the workplace. This is a dangerous argument. In the mid-nineteenth century in Britain, a group of factory owners, who were called somewhat uncharitably by Dickens as "*The Association for the Mangling of Operatives*", banded together to oppose various laws designed to improve workplace safety, on the grounds that workers had chosen their jobs of their own freewill in the understanding of the hazards involved (i.e. the risks were voluntary). However, the view prevailed that people, whether at work or elsewhere, should not be exposed needlessly to hazards. There was a duty of care.

Whether any risk is acceptable is a matter of debate. For that reason, some authorities prefer to speak of *tolerable risk*. Following an inquiry into the siting of a nuclear power station, Sizewell B, the United Kingdom's Health and Safety Executive[12] commented:

> *"Tolerability" does not mean "acceptability". It refers to the willingness to live with a risk to secure certain benefits and in the confidence that it is being properly controlled. To tolerate a risk means that we do not regard it as negligible or something we might ignore, but rather as something we need to keep under review and reduce still further if and as we can.*

Table 3.1 illustrates that we fear the unknown hazards, particularly those that are perceived to have lingering or life-threatening effects. We are also averse to situations where harm can happen to a large number of people simultaneously. We appear to view more seriously the multiple deaths in a single air mishap than the same number of fatalities spread over our roads in separate accidents. The November 1979 crash of a commercial aircraft on a sightseeing overflight in Antarctica put the whole country into mourning, even though the loss of life was less than half that of the annual road toll.

Risk Characterisation

In a book entitled "*Understanding Risk*", the National Research Council of the United States[13] notes that coping with risks can be both complex and controversial. One of the reasons the authors cite for this situation lies in the misconceptions in characterising risk. From an engineering viewpoint, risk may be characterised as a result of a technical analysis of likelihood and consequence, which is then used as an aid in decision-making. The National Research Council, however, see risk characterisation as a wider process, in which the results derive from both analysis and deliberation.

Therefore the aim of risk characterisation is considered to be this *dual process* of describing a perceived hazard in a way that addresses the significant con-

cerns of all interested and affected parties in a manner understandable to them. In the language of the Risk Management Standard, *a risk cannot be fully characterised until it is communicated and "accepted*". This implies that coping with any risk requires a broad understanding of the possible consequences to all the stakeholders. As noted in this Standard, the final decision about a risk is the result of a stepwise process involving consultation at the various stages from perception to treatment.

Nevertheless, in many areas of technical safety, the public has trusted professional engineers and regulatory authorities to exercise responsible risk management with the minimum of consultation. Earthquake engineering and airline safety are examples of two areas where few citizens understand and have commented on the technologies that have reduced risk levels over the years. Generally, public concern has concentrated on engineering activities that impinge on lifestyles, such as motorway construction, and the management of perceived risks to the environment through the release of contaminants of various kinds.

References

1 McNamee, D and Selim, G (1998): *"Risk management: Changing the internal auditor's paradigm"*, Inst. Internal Auditors Res. Found., Altamonte Springs, FL.

2 Elms, D G (1998): "Overview - Prudence, principles and practice", in Elms D (ed.) "I*ntegrated Risk Management in Practice*", CAE , Christchurch.

3 Lees, F P (1996): "*Loss Prevention in the Process Industries*", 2nd edn, Butterworth-Heinemann, London.

4 Rutstein, R and Clarke, M B T (1979): "Probability of fire in different sectors of industry", F*ire Surveyor*, 8(1), 20

5 Mahoney, D G (ed) (1990). *"Large Property Damage Losses in the Hydrocarbon-chemical Industries"*, 30th edn., M&M Protection Consultants, New York.

6 Merrison, A W (1971): *"Inquiry into the basis of design and method of erection of steel box girder bridges"*, HMSO, London.

7 Keey, R B and Smith, C H (1984): "The propagation of uncertainties in failure events", *Reliab. Engng*, 10, 105.

8 Kletz, T A (1999): "*Hazop and Hazan*", 4th edn, IChemE Rugby.

9 Kletz, T A (1995): "Improving organisations' memories", *IChemE Loss*

Prevent. Bull. (124), 20-1.

10 Suter, G W (1993): "*Ecological Risk Assessment*", Lewis, Chelsea MI.

11 Lowrance, W W (1976): "*Of Acceptable Risk*", W Kaufmann, Los Altos, CA.

12 Health and Safety Executive (1988): "*The Tolerability of Risks from Nuclear Power Stations*", HMSO, London.

13 Stern, P C and Fineberg, H V (eds)(1996). "*Understanding Risk: Informing Decisions in a Democratic Society"*, Nat. Acad. Press, Washington, DC.

Nature of risk

4 Risk Identification

Risk identification needs to be a well-structured, systematic process. The identification of a risk begins with a perception of a hazard, a threat to people and the things they value[1]. A particular hazard may pose different threats to different people and in different contexts. The threat may be evaluated not only in physical terms but also by factors such the credibility and trustworthiness of risk management and any regulatory bodies. While an engineer may describe a risk in numerate terms of probable incidence rates and extent of physical damage should the hazard eventuate, others will use informal and social criteria to judge the threat.

We can no longer talk with any confidence about determining *objective* risk. "*Social, cultural and political processes are now acknowledged as all being involved in the formation of individual attitudes to risk*"[2]. All assessments of risk involve subjectivity to a greater or lesser extent, since the process of identification depends upon subjective judgments on what constitutes a risk. Engineers and others often have the greatest difficulty in resolving disagreements on this point.

Risk Context

The Australian/New Zealand Risk Management Standard states that the identification of risks must take place within a given context. Defining this background and framework is the first step in any risk study, setting the parameters for its scope. The context is specified by the nature of the organisation undertaking the risk study, its capabilities, goals and strategies, as well as the organisation's relationship with its environment. Previous generic studies of risk and case histories may provide a guide for defining the scope. Appendix D of this Standard lists generic sources of risk and areas of impact which can serve as a starting point. A summarised version in given in Table 4.1.

Risk Perception

Establishing the context involves awareness and knowledge of a potential hazard. Understanding that there is a potential risk includes psychological, social and ethical aspects. Different societies will choose different risks to be concerned with, and the set of concerns will change with time. Different people may choose different boundaries of risk. Gough[3] cites the case of the perceived hazards of a proposed LPG storage depot at Seaview near Wellington. The company considered only the site-related hazards in its environmental impact report, whereas some local residents wanted consideration of the complete

Table 4.1: Generic sources of risk and their areas of impact (adapted from Appendix D, AS/NZS 4360:1999)

Sources of Risk	Principal Areas of Impact
Commercial and legal relationships	Asset and resource base
Economic circumstances	Revenue and entitlements
Human behaviour	Costs and people
Natural events	Costs and people
Political circumstances	Community and operation
Engineering and technology	Costs and performance
Management activities and control	Costs, performance and reputation

Note: the sources of risk may impact on all areas

transportation system for LPG within the metropolitan area as well. Changing the area of concern revealed a different set of potential hazards.

Hazards that are likely to give rise to particular concern to people are those that pose, or seem to pose threats to their valued cultural and social arrangements. Examples in the New Zealand context might be possible pollution of customary fishing grounds or the disturbance of sacred sites. Such perceived risks cannot be explained by individual psychology, or dismissed through the quantitative analysis of so-called "objective" risks which tries to demonstrate that the "real" risks are very small.

The perception of potential hazards also involves judgments about the ongoing risk management. Risk-management policies can alter, following corporate restructuring and political change. Such changes are normally carried out for specific organisational motives and philosophies without any or with little consideration of the safety implications. Safety standards can slip. This may happen, for instance, when a corporate change places less reliance on in-house expertise for maintenance, on the assumption that consulting services collectively have the same knowledge of the particular engineering systems.

With manufactured and processed goods, the risks change from the time of manufacture, transport to points of sale, subsequent use and final disposal. The hazards of a pesticide are an example. The risks during production in the process plant under carefully controlled conditions are likely to be much less than the risks while spraying in the open air, when drift and eddying of the spray mist may occur, and operators may be tempted to work under less than ideal conditions. Furthermore, risks during production are different from the risks of dumping any unwanted or unused material. *In such cases, careful consideration must be given to the scope of the study to reveal all relevant risks* and so save considerable time and effort in remedial work later on.

If the precautionary principle is adopted, and hazards are assumed to exist until

proven to be absent by further knowledge, the boundaries of our concern are clearly crucial in our risk assessment. The question is: who and what are at risk? Professional engineers and others who claim expert knowledge can easily fall into the trap of believing that they instinctively understand all the risks and their associated causes. The use of the Australian/New Zealand Standard and a generic checklist, such as Table 4.1, offers a very good guide to the perception and identification of risks that might easily have been overlooked in the first instance.

Case Study 4.1 Stadium Construction Risk Analysis
(Bermingham, 1999, *pers. comm.*; courtesy, Wellington Regional Council)

The Regional Council had agreed in principle to support the building of the WestpacTrust Railyards Stadium by way of a substantial loan. They considered it prudent to have an analysis of the construction related risks carried out prior to finally committing to the project.

As the time scale was tight, a small team of experienced engineers was assembled and a semi-qualitative methodology applied. Using the hazard identification approach suggested by AS/NZS4360, and under the guidance of a risk engineer, they rapidly identified the major sources of risk. Local knowledge and professional experience were used to judge the likelihood and significance of each potential event. A simple scale was used to value and rank these. This listing was used to identify the higher risks and to obtain comment and, where necessary, improved mitigation plans from the project management team.

The study identified a range of risks that had not formerly been considered and facilitated the development of a range of mitigation measures that significantly reduced construction-related risks.

As controls were put in place to manage each significant risk and as the overall residual risk was considered acceptable, WRC were able to commit to the project with more certainty that the project would meet the success criteria.

This is a good example of how even a simple risk-based approach can aid management decision-making. In particular it shows how AS/NZS 4360 can be effectively and quickly applied without the addition of sophisticated techniques or in-depth research.

Accident Causes

Organisations of all kinds are increasingly being required to demonstrate, internally and externally, that they are systematically controlling occupational health and safety hazards. There has been recent public concern at the rate of industrial accidents in New Zealand. In the United Kingdom, the Health and Safety Commission issued, in early 1999, a discussion document on proposals to introduce a new duty on employers to investigate the cause of workplace accidents.

As equipment has become inherently more reliable and safer, attention is now being focussed on the human causes of accidents. Lucas[4] recognises four underlying ideas or paradigms of human behaviour that give rise to errors, as set

out in Table 4.2.

Table 4.2: Error paradigms of human behaviour (after Lucas[4])

Error paradigm	Basic Assumptions	Solutions
Engineering error	People are the unreliable component in the system	Remove people from the system by automation
Individual error	Poorly motivated people commit unsafe acts	Discipline those involved
Cognitive error	A mismatch between individual capabilities and the demands of the job	Ensure job and workload can be done
Organisational error	Poor management create conditions that make errors likely	Examine and audit management systems

All of these error paradigms contain elements of truth, but the uncritical adoption of one paradigm to the exclusion of others is likely to lead to root causes of some accidents being missed. This point is perhaps illustrated by the differences in opinion in investigating the cause of the DC10 aircraft that crashed in Antarctica in November 1979 on a sightseeing flight. The then Chief Inspector of Air Accidents attributed the cause to pilot error. The subsequent inquiry of the Royal Commission under Mr Justice Mahon took a wider view, and considered related systemic issues, including the impact of other factors that could have led to a dangerous situation occurring (such as lack of charts showing a printed route).

Root Causes

As many inquiries have observed, a technical hazard is often triggered through root causes that are non-technical in origin. Most formal risk-identification methods are concerned with finding technical risks, and thus it is always important to confirm that technical standards are not compromised by other factors. A checklist of underlying or systemic errors can assist in pinpointing possible latent parameters.

Wells[5] gives a list of these deficiencies, which may be used to confirm that adequate engineering and administrative controls are in place. Such root causes include:

- Deficiencies in external agencies such as contractors and emergency-response providers;
- Deficiencies in the regulatory climate;
- Any harmful influence of economic factors and business focus;
- Lack of adequate corporate commitment to safety and emergency provision;

- Poor management control, including responsibility for engineering matters;
- Poor site and plant facilities including site layout and the transport, storage and disposal of materials;
- Poor communication, including safety information and incident reporting;
- Poor working practices and emergency procedures;
- Poor working environment, including welfare, supervision and support;
- Poor engineering integrity, including the quality of plant, its availability and maintenance;
- Poor performance of workers, including aspects such as their training and work habits.

There are numerous root causes, and systems must be set up to guard against them and monitor safety performance.

Large organisations involved with activities of high hazard potential normally have whole departments whose sole task is the monitoring of safety trends and the analysis of incidents including so-called "near-misses". Such departments are continually trying to identify root causes and checking whether any previous risk-assessment work has not been compromised by environmental, operational, technical and organisational changes. However, even small organisations should be on their guard. Routine inspections, say monthly, checking aspects such as equipment availability, minor defects (such as leaking valves and indicator faults on process plants) and site tidiness comprise one such system. Kinsman[6], from experience in the United Kingdom, reports that there can be a twentyfold change in reliability of process plant as a result of the way in which it is managed.

Early Hazard Identification

At the start of a engineering project, when the technical and economic evaluation of the project's feasibility is being done, and the criteria for success are being set, an assessment of the safety, health and environmental (SHE) hazards associated with the proposals should be undertaken. This initial SHE study is a core component of policy decisions such as siting and, in the case of an industrial facility, the preferred manufacturing and process arrangements. Subsequently, a *concept hazard analysis* would be done to identify areas that may present unacceptable risks.

The initial study would consider all the organisational factors affecting the project, including the need for and the availability of experienced workers and technical staff in both the constructional and operational phases of the project.

Table 4.3: Keywords for concept hazard analysis in regard to human safety (after Wells[5])

Fall of person from height	Drowning
Fall of object/material from height	Excavation work
Fall of person on same level	Stored energy
Manual handling	Chemical / dust explosion
Mechanical lifting operations	Contact with cold/hot surfaces
Compressed air	Chemicals/substances
Use of machines	Biological agents
Operation of vehicles	Noise
Stacking	Ionising radiation
Housekeeping	Non-ionising radiation
Lighting	Vibration
Fire, including static electricity	Handtools
Electricity	Confined spaces
Adverse weather	Cleaning

General project criteria should be set, including the codes of practice to be followed and any regulatory standards to be met.

The concept hazard analysis would draw in appropriate specialists who would discuss various aspects of the project at a series of meetings. A checklist, such as Table 4.1, could be used as a framework to enhance the chance of identifying all significant hazards. Various keywords might be used to stimulate discussion. In regard to human safety, Wells[5] has produced a list of suitable keywords based on information published by the British Institution of Occupational Health and Safety. This list is reproduced in Table 4.3.

Under New Zealand conditions, one would add the keyword "earthquake", and each industry or engineering activity would doubtless generate its own particular set. The technique has been developed for a proposal which involves a sequence of activities, as in a manufacturing or process plant, with each section being considered in turn, but can be adapted to any kind of engineering works. Because the technique is applied at an early stage of a project, recommended changes can be made easily with little cost, and with potential long-term savings in avoiding the need for add-on safety measures at a later stage.

Wells[5] illustrates the methodology with an example of a lifting problem. A container holding a dangerous material on a flatbed trolley was to be lifted by an overhead crane over a 6m high wall into a building through a ventilation space. Under the keyword, *drop/impact*, the team decided that there was a hazard if the container were dropped from a height greater than 5m, and recommended that the wall be reduced in height, with a roller shutter to close off the

larger hole in the building. The operation would then be inherently safer.

Sometimes a preliminary hazard identification is all that is needed, as illustrated in Case Study 4.1.

Identification of Major Hazards

Major hazards, with potentially far-reaching impacts, are generally those which relate to the dangerous properties of a material being made, stored or used at a particular site and in the transport of such material. The size of the inventory and the state conditions of temperature and pressure will determine the consequence of the release of materials and energy into the environment. Flammable liquids stored under pressure at temperatures above their boiling points are particularly hazardous as any released liquid will flash into vapour, with the chance of fire and an explosion. The same liquid, at a temperature below its boiling point, has much lesser chance of catching fire as there is considerably less vapour formed when the material escapes.

Chemical hazards are not necessarily confined to the chemical-process industries. McKay[7] describes a safety audit on a large microelectronics factory in Hong Kong which employed 2500 people and covered an area of 60 000 m^2. The facility manufactured microchips on wafers in a very clean environment and a number of hazardous liquids and gases were handled on site.

Bretherick's handbook[8] is a source of information on reactive chemical hazards. A substance may release energy by either combustion or decomposition. A very rapid energy release (as in a detonation) can occur if the carbon and hydrogen in a substance can react with its own oxygen without the need for any oxygen in the air. The oxygen balance in a compound is an important indicator of its stability. This quantity *OB* is defined for an organic compound of formula $C_xH_yO_z$ as:

$$OB = -1600(2x + y/2 - z)/M$$

where M is the molecular weight. An unstable compound with a perfect oxygen balance, yielding just carbon dioxide and water, would have an *OB* value of zero, and one containing excess oxygen a positive value. Compounds with large positive (>240) and large negative (<-160) values are considered to have a low energy-hazard potential[9].

The heat of decomposition ΔH_d is also a factor in the hazard potential. This is considered low should

$$\Delta H_d^2 M < 50$$

where the heat of decomposition ΔH_d is measured in units of MJ/kg.

One of the commonest operations in the process industries is heating a wet

material to drive off moisture to yield a dry product. Most products of animal or vegetable origin are combustible, and the drying of these materials can lead to fires and dust explosions. The frequency of problems in the spray drying of milk powders triggered a review of industrial practice in New Zealand, with the formulation of a code of practice (1987) to enhance safety.

Most household products involve hazardous materials in their manufacture; inherently, most process chemicals are chosen because of their reactivity and aggressive properties. Toxic chemicals can enter the body in three ways: through breathing, by ingestion or by external contact. The effects of exposure may be *acute*, resulting from a single exposure to a high concentration of the toxic material, or *chronic* from a low-level exposure over a long period. Some substances, such as hydrocarbon vapours have narcotic effects; some gases are asphyxiants, displacing or blocking oxygen to the lungs; other chemicals can induce tissue damage or induce cancers and gene changes, with different organs being effected by different chemicals. Some chemicals accumulate in the body; others can be expelled harmlessly. Thus it is difficult to describe the toxicity of chemicals on some kind of common scale. There are, however, comprehensive accounts of toxic hazards, such as Sax's "*Dangerous Properties of Industrial Materials*"[10].

New Zealand has been spared a catastrophic incident like the accidental release of methyl isocyanate at Bhopal, but the so-called Parnell fumes emergency in 1973 was an example of the far-reaching impact of an escaping toxic vapour on an unsuspecting population. Thirteen damaged and leaking drums containing an unknown agricultural chemical had been offloaded from a freighter and had been dumped overnight on a vacant section pending a decision for their disposal. Soon neighbours began to complain of sore throats and smarting eyes, and the Fire Brigade was called; within a short time, people over a wide area began to feel ill. Over the five days it took to bring the emergency under control and decontaminate the site, 643 people had been admitted to hospital and 6000 persons had been evacuated. Fortunately, there were no deaths, and most people recovered within 12 to 24 hours[11].

Lees[12] summarises various screening tests that can be done to assess material-related hazards. There is also a range of hazard indices that have been developed: these are considered in Chapter 5 under short-cut methods of risk analysis.

OSH Method of Hazard Identification

On the introduction of the Health and Safety in Employment Act 1992, the Department of Labour issued a workbook, "*How to Identify and Control Hazards*" (1992). This guide advocated three ways to identify systematically existing hazards in the workplace:

1. By examining specific areas of the worksite and the activities carried out

in them;

2. By analysing different occupations and their tasks;

3. By analysing the total process used to convert raw materials into the final product for sale.

By area. From an up-to-date plan, the worksite is divided into distinctive areas (such as workshops, yards, stores and various production areas). Staff familiar with the particular areas are then asked what they consider to be the hazards or potential hazards of those areas. It is suggested that records of accidents and illnesses, relevant codes of practice and any existing safety audits or environmental-monitoring reports be used to assist assembling the list of hazards.

By worktype. Work that is not associated with one location is better analysed by identifying the different occupations involved, and noting the hazards that are faced as the work is carried out. This method is particularly relevant for tradespeople who might be required to service a range of items throughout the whole site. It would also be suitable for analysing the hazards faced by gangs of workers, as in forestry, who operate in small autonomous groups with minimal supervision. Accident records and anecdotal tales of near-misses could be used to build the profile of hazards.

By process. This method follows the process of production, step by step, trying to identify the hazards at each step. It involves listing the progress of each raw material to the site to the points where the goods are dispatched, identifying the places where material is transformed by physical, chemical or biological means, and noting the hazards associated with these transformations. The technique differs from a hazard and operability study (Hazop), which is a detailed examination of process deviations, section by section on the plant.

Although the OSH method was developed as a technique to identify workplace hazards, the methodology can be more generally applied, as illustrated by the study by Boyes[13] of the risks of associated with a cargo port over its lifecycle from construction to decommissioning. Other categories of risk that might be used in an OSH-type analysis includes factors such as: *activities*, *assets* and *location* (both from the built and the natural environment).

Workplace-risk management is discussed further in Chapter 8.

Hazard and Operability Study (Hazop)

Hazard and operability studies (Hazop) had their origin in the chemical process industries in the 1970s as a response to increasing problems in bringing large process plants onstream. In this regard, the methodology was successful. Knowlton[14] reports that over an eight-year period in which all new plants were subject to a Hazop scrutiny, the average time between start-up and the achieve-

ment of full output was one month, compared with three months for plants for which no such study had been undertaken.

A hazard and operability study is suitable for any manufacturing or process facility in which deviations from normal working conditions may occur. It is not a trivial undertaking, although it has gained wide acceptance from industry because it does not require sophisticated reliability calculations. Essentially, it is a formal method of aggregating the experience of a number of people with intimate knowledge of aspects of the facility under review.

Keey[11] summarises the methodology. The composition of the review team will depend upon whether a new design or an existing plant is being considered. In either case, an accurate and complete process flowsheet (such as P&I diagram) is required, because this is the basis on which the plant's behaviour under conditions away from normal will be judged. A team leader then takes the group systematically though the plant, which is broken down into elements that have a single function, such as a pump and associated pipework feeding a vessel from another tank. A series of check or guidewords are then applied to each of these elements in turn: none; reverse; more of; less of; part of; other than. The first guideword, when applied to the pipeline, means no forward flow when there should have been flow. The team would then ask itself:

- Could there be no flow?
- If so, how could it happen?
- What are the consequences of no flow?
- Are the consequences hazardous and do they hinder effective operation?
- If so, does the size of the hazard or the operability problem justify the expense of rectifying it?

The team then considers what happens if there is reverse flow, and so on. The deviations triggered by various guidewords are listed in Table 4.4. The various conclusions are recorded by the team leader, listing the points of action noted, which are followed up. Because the concentration of team members can lapse after a period, it is normally recommended that Hazop exercises are limited to sessions of no more than two hours duration.

Although Hazop was originally conceived as a qualitative review, the results can be quantified to some extent by simple ranking of likelihood (or frequency) and severity (or consequence) to give a risk matrix. Examples of such ranking methods are considered in Chapter 5.

The effectiveness of the technique can be improved by paying attention to psychological factors in the selection of participants for Hazop meetings and how those individuals within that group perceive, remember, judge and reason.

Table 4.4: Deviations generated by guidewords in Hazop (after Kletz[17], with modification)

Checkword	Deviation
None	No flow when there should be
Reverse	Reverse flow to that intended
More of	More of the relevant property (flow, pressure, temperature) than there should be
Less of	Less of the relevant property (flow, pressure, temperature) than there should be
Part of	Composition different from what it should be (components missing, proportions different)
More than	More components present than there should be (impurities, extra phase)
Other than	What else can happen away from normal working: at start-up, shut-down, low running, overload, failure of services, during maintenance checks

Leathley and Nicholls[15] review aspects such as the improvement of corporate memory, the enhancement of creativity and the retention of attention span.

Skelton[16] provides a listing of the causes of some of these deviations. For example, no flow may be the result of a wrong routing of material, a blockage, the incorrect insertion of a slip-plate in the line, an incorrectly-fitted non-return valve, a large leak from a burst pipe, a valve wrongly isolating the line, a vapour lock, and through no material being available(!) Clearly, the success of any Hazop exercise is very dependent on getting together a team with sufficient breadth of experience to foresee all the potential causes. It is also necessary to work from correct, up-to-date diagrams. A Hazop study on a wrong section or an outdated one is useless!

Lees[12] gives examples of a number of Hazop exercises from the process industries, including the application to batch operations when time is an additional factor to be taken into account. Hazop methods have been used extensively in New Zealand in the assessment of the safety and operability of new process engineering facilities and other industrial plant.

Failure Mode and Effects Analysis (FMEA)

A Failure Modes and Effects Analysis (FMEA) involves the consideration of the possible outcomes from the discerned failure modes within a whole system. It is particularly suited to electrical and mechanical systems, and can be applied at different levels of detail or complexity. At an initial broad level, it provides insight into the most important or critical contributing factors that can be ana-

lysed in further detail.

The method consists of identifying the failure modes, their causes and effects, their relative importance and sequence, for the system to be evaluated, and the way in which these failures will be detected, rectified or isolated. As with Hazop, a listing of effects and appropriate corrective action is produced. The analysis can be either function or hardware-based, and the study can be combined with approximate quantitative measures of fault frequency to identify critical components that govern the reliability of the whole system. The method, however, relies on the skill of the analyst in having a thorough understanding of the workings of the system. Wallace[18] also notes that this method of analysis may not give adequate emphasis to omissions or errors in operating procedures, incorrect operational sequences in batch operations, or the possibility of operator's errors.

Guidance on the use of failure mode and effect analysis is given in BS 5760 *Reliability of Systems, Equipment and Components*, Part 5:1991 *Guide to Failure Modes, Effects and Criticality Analysis*. Two examples of the application of the methods are given in that document: the analysis of the fire-protection system of an electric locomotive and the reliability of a subsystem of a motor-generator set.

Artificial Intelligence

The development of computer-aided design has led to consideration of the possibility that hazards might be identified through artificial intelligence techniques[19]. Most proposed systems developed follow a Hazop-type screening in which the examination moves systematically though a plant, line by line. There is currently some scepticism about the efficacy of such software, as it is difficult to compete with human ingenuity in thinking laterally and making connections which appear obscure at first sight. One interesting approach is the HAZID code developed by Parmar and Lees[20], in which a Hazop-type approach is used together with generic information on fault-propagation pathways.

Other Methods of Identification

What-if analysis. This is perhaps the oldest method of identifying a technical hazard. The technique consists of asking questions such as:

- What if the electrical power fails?
- What if the pump stops?
- What happens in an earthquake?

The method is used against a checklist by a team, and is useful in an initial review of a proposal as part of a concept hazard analysis.

Sneak analysis. This method originated in the analysis of electrical circuits when it was discovered that unsuspected or "sneaky" current flows to earth sometimes occurred because of design errors in circuitry[21]. There are various kinds of sneaky faults. A "sneaky" signal happened on the nuclear power plant on Three Mile Island at the time of the emergency. There was an indication of "valve position", which was the signal to, rather than the actual position of a power-operated relief valve. A "sneaky" flow can take place from one vessel at higher pressure to another at a lower pressure through a common header that is normally shut. At Seaview near Wellington, there was a "sneaky" separation of an oil-water emulsion during an atypical shut-down of a plant, which led to a steam explosion when the plant was started up again and the mixture reheated.

A good plant engineer is always on the lookout for unusual and unintended pathways. The original sneak-analysis method involved decomposing an electrical network into standard subcircuits for which the current flows could be determined. The method can be applied to a process network by analogy, by representing the system as a series of sources and sinks with interconnecting pathways. An additional technique is the use of "clues" from a structured checklist to search for misleading labels and indication of plant status and other unsuspected equipment behaviour.

The principles of a sneak analysis may be used to enhance a Hazop exercise[22]. In the reported study of a large batch plant, a number of "sneaky" faults were picked up, including: wrong labelling, misleading indicator lights, two major drawing errors, drainage problems, improper coupling to the fume-extraction system, and numerous false procedures.

The common and most important theme that comes through the various methods is that *effective risk identification must be systematic*. Otherwise, when a subsequent analysis of the risks is undertaken, the assessment will be devalued by the failure to encompass all the hazards in the study.

Hazards of Safety Systems

Unwittingly, a designer specifying a safety device may introduce another hazard. This may arise when, for example, a trip system responds spuriously. Kletz[23] cites the case when several people nearly drowned in the deluge from water sprays which were set off falsely inside a containment building of a nuclear-power plant. Both "*fail-danger*" and "*fail-safe*" incidents have to be considered in assessing the hazard potential of any facility. Another example of the potential by-hazards of water sprays was the initial requirement, placed on one metallurgical laboratory in New Zealand which housed a steel-melting furnace, to fit overhead sprinklers for fire-safety precautions.

Modifications to equipment to meet particular deficiencies in performance can also lead to the development of unsafe systems if the modified arrangements

have not been assessed for possible hazards, say through a failure modes and effects analysis. Informal changes can often result in a chain of modifications until a final satisfactory solution is found.

References

1 Kates, R W and Kasperson, J X (1983): "Comparative risk analysis of technological hazards", *Proc. Nat, Acad. Sci. USA*, 80, 7027-7038.

2 Pidgeon, N, Hood, C, Jones, D, Turner, B and Gibson, R (1992): "Risk perception", in "*Risk: Analysis, Perception and Management*", 89-134, Royal Society, London.

3 Gough, J D (1990): *"A review of the literature pertaining to 'perceived' risk and 'acceptable' risk and the methods used to estimate them"*, Inform. Paper no. 14, Centre for Resource Management, Lincoln

4 Lucas, D (1997): "The causes of human error", in Remill, F and Rajan, J, "*Human Factors in Safety-critical Systems*", Butterworth Heinemann, Oxford.

5 Wells, G (1996):"*Hazard Identification and Risk Assessment*", IChemE, Rugby, UK

6 Kinsman, P (1991): "*Major Hazard Assessment: A Survey of Current Methodology and Information Sources*", HSE Rep. No. 29, UK Health and Safety Exec., London

7 McKay, G. (1999): "Designing a process hazards analysis methodology for a "non-traditional" chemical facility", *IChemE Loss Prevention Bull.* No 147, 22-6.

8 Bretherick, L (1990): *"Bretherick's Handbook of Reactive Chemical Hazards*", 4th edn, Butterworth Heinemann, London.

9 Treeweek, D N, Calydon, C R and Seaton, W H (1973): "Appraising energy hazard potentials", *Loss Prevention*, 7, 21.

10 Sax, N I (1989): "*Dangerous Properties of Materials*", 7th edn, van Nostrand Reinhold, New York.

11 Keey, R B (1987): "*Reliability in the Process Industries*", IPENZ, Wellington.

12 Lees, F P (1996): "*Loss Prevention in the Process Industries*", 2nd edn, Butterworth-Heinemann, London.

13 Boyes, W J (1998): *"Risk assessment for a port proposed at Marsden Point by Northland Port Corporation"*, BE (Chem. & Proc.) Rep., Univ. Canterbury, Christchurch.

14 Knowlton, R E (1981): "*An Introduction to Hazard and Operability Studies: The Guide Word Approach*", Chemetics International Ltd, Vancouver, BC

15 Leathley, B and Nicholls, D (1998): "Improving the effectivenes of Hazop: a psychological approach", *IChemE Loss Prevention Bull.*, no. 139, 8-11.

16 Skelton, B (1997). "*Process Safety Analysis - An Introduction*", IChemE, Rugby, UK

17 Kletz, T A (1985): "Estimating potential hazards", *Chem. Eng.*, 1 April, 48-68.

18 Wallace, I G (1995): "*Developing Effective Safety Systems*," IChemE, Rugby, UK.

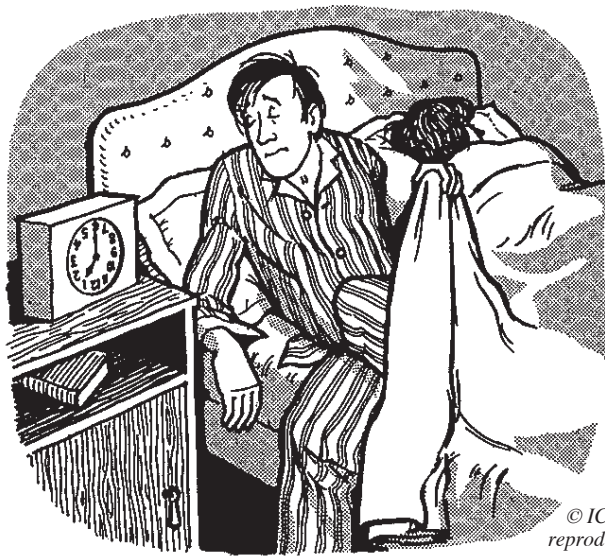
19 Ferguson, G and Andow, P K (1986): "Process plant safety and artificial intelligence", *Proc. World Cong. III Chem. Engng*, Tokyo, 1092.

20 Parmar, J C and Lees F P (1987): "The propagation of faults in process plants: hazard identification", *Reliability Engng*, 17(4), 277.

21 Hill, E J and Bose, L J (1975): "Sneak circuit analysis of military systems", *Proc. 2nd Internat. Systems Safety Conf.*, 351- 372 [reported by Whetton (1993)].

22 Whetton., C P (1993): "Sneak analysis of process systems", *Process Safety and Environ. Protection*, 71(B3), 169-179.

23 O'Mara, R L and Bergeron, C B (1987). "Inherent safety - how to keep a new safety system from causing an accident", cited by Kletz, T A (1999), "*Hazop and Hazan*", 4th edn. IChemE, Rugby, UK.



5 Risk Analysis

The Australian/New Zealand Risk Management Standard describes the objectives of risk analysis as the separation of minor acceptable risks from the major risks, and to provide data to assist in the evaluation and treatment of risks. Risk analysis is the process to determine the remoteness of identified hazards and the possible consequences should they happen. Often a preliminary analysis is carried out so that similar or low-impact risks are excluded from a detailed study. The Standard emphasises that excluded risks should, wherever possible, be listed to demonstrate the completeness of the risk analysis.

At its most elementary form, the analysis may be a qualitative estimate in terms of verbal descriptors such as "likely" or "improbable". However, if appropriate data are available, it can involve sophisticated calculations to follow fault-propagation pathways and computer-aided modelling for various scenarios of specific realised hazards. Such calculations are desirable in cases where realised hazards are perceived to have a high impact, such as the high-pressure storage of flammable liquids. In general, engineers will invariably need to carry out risk analyses in more detail than many other professions, as reflected in the analytical methods developed for engineering use such as fault-tree analysis.

Such calculations are subject to significant uncertainties. One aspect of this uncertainty is the need, at times, to make subjective engineering judgments about the behaviour of equipment and people in emergencies and when failures arise. Such subjective judgments incorporated in ostensibly objective calculations are highlighted by the occasional (and embarrassing) attempts to compare predictions of technical experts. Hynes and Vanmarche[1] asked seven internationally known geotechnical engineers to estimate the height of an embankment that would cause failure in a clay foundation. They were asked to set confidence limits on their estimate wide enough to have a 50% chance of enclosing the true height, None of the engineers, it was reported, were able to establish limits that enclosed the true height!

Dunster and Vinck[2], in weighing up the value of risk analyses in the nuclear industry, have commented:

> *"Uncertainties in estimates of probabilities of events by factors of less than two or three can hardly be expected, and uncertainties by a factor of ten or more may well occur, even in carefully conducted studies. The estimation of the magnitude of the consequences in human terms almost always involves environmental modelling and similar factors of uncertainty are to be expected."*

Although such uncertainties have cast serious doubt in lay minds about the value of these numerical estimates, risk calculations do provide a basis for ranking alternatives and comparison against risk-target levels when often order-of-magnitude estimates are good enough. Moreover, in determining the impact of far-reaching accidents, an order-of-magnitude uncertainty in incidence may correspond to a much smaller uncertainty in the hazard, as the effects of many mishaps (such as fires) dwindle rapidly with distance. Careful use of group judgments, with professional consultants when appropriate, can in many cases achieve worthwhile results and amplify limited or missing historical data.

Risk analysis is a tool, but like all tools, must be used appropriately and with skill. Occasionally practitioners have been carried away by the methodology. The Comptroller-General's 1978 report to the US Congress drew attention to one study of risks in the handling of liquefied natural gas in which an estimate of an annual probability of 5×10^{-50} was given for a particular event that might kill 100 000 people! In one New Zealand study aimed at setting town planning guidelines for the siting of industries with a perceived high hazard potential, the maximum number of offsite fatalities from material-related hazards at the edge of an industrial zone was estimated to be 8 for an event of frequency of 1 in 10 million years[3]. One suspects that there may have been other hazards arising from such industrial activity which were of greater concern to the neighbouring residential area, subject to significant seismic risks with a high probability of being observed in a person's lifetime.

Yet "highly improbable" events do occur. Bond[4] tells the story of the unfortunate Major Walter Summerford whose experience with lightning was most extraordinary. He was struck by lightning on a battlefield in Flanders in 1918, and was invalided out of the army. In 1924, while in Canada, he was again struck by lightning, and yet again in 1930, which left him paralysed. In death, he was not left in peace: his gravestone was stuck by lightning and was destroyed. *Doubtless a risk analyst could estimate the very low probability of this sequence of events!*

Early failures

Experience with the reliability of engineering components and systems leads us to judge an expected life for these based on some mean time between failures. If any failure occurs well within this mean life-span, we tend to say that the failure is "unexpected". However, even if failures occur randomly, there is always a chance of seeing an "early failure". Suppose, for example a component has an expected life of 5 years. Should failures be random over this period, the probability of failure P_f at any time t/ yr is given by the expression[5]

$$P_f = 1 - \exp(-t/5)$$

so that at the end of the first year of operation the probability of seeing a failure is 9.5%, which is small, but not negligible. Half-way through its expected life the failure probability has risen to 39%.

The likelihood of early failure has important implications whenever a high degree of reliability is sought. The comment that the four electrical cables feeding the central business district of Auckland in early 1998 failed "well within their reasonable expected lifetimes" was no consolation to the power company's customers who were expecting an unbroken supply of power. Reliability, in such circumstances, has to be secured through adequate redundancy and loss-prevention management. Modern risk management provides the opportunity to foresee problems of unreliability and plan to reduce and cope with the likelihood of such failures.

Unfortunately, early failures may not be entirely random events. Although early failure of industrial equipment is sometimes perceived as due essentially to the breakdown of weak or substandard components, there are other factors. Sherwin and Lees[6], for example, have found early failure prevalent in both process-plant equipment and hospital autoclaves. In both cases, problems with maintenance work and a lack of training appeared to be the main cause. Improvements in maintaining the autoclaves, after certain recommendations had been made, resulted in a fourfold reduction of the overall failure rate. This example cannot be considered to be an isolated case. Experienced plant engineers, on diagnosing a defect, will normally ask whether maintenance work had been recently carried out on the faulty item.

OSH Risk-rating Method

The Occupational Health and Safety Service (1992) has suggested a process to evaluate each identified hazard in the workplace, so that a decision can be made on whether

- Injury or illness could result from it; and if so;
- What action need be taken to reduce the risk.

This process is seen as a means of planning, introducing and monitoring risk-control measures to meet statutory requirements under the 1992 Act.

For each identified hazard, the possibility is considered of injury, illness or damage which might result from the hazard should it happen. The next steps involve setting a potential severity rating (on a five-point scale from negligible harm to possible death(s)) and a probable frequency rating (on a four-point scale from "remotely possible" to "happening all the time"). A risk-rating value is obtained by multiplying the severity and frequency ratings.

The method provides an approximate means of ranking hazards in their impact. It relies on prior experience of the hazards being assessed and is difficult to apply when new technology is involved. Furthermore, different combinations of frequency and consequence can yield the same hazard score, but the risks may not be equal in significance. It is thus only a guide in ranking. However, it can be a very useful tool in a scoping study of possible hazards, as Case Study 5.1 demonstrates.

Case Study 5.1 Harbour Extension[31]

Because of limitations of the existing facilities in Whangarei harbour, Northland Port Corporation has considered a possible port extension of 50 ha, of which 32 ha would be reclaimed land for open storage obtained by dredging a ship-turning basin. A scoping study to identify the hazards associated with the proposed development was undertaken to cover all phases in the operation of the port from construction, working life and possible final disuse. Besides the hazards of handling cargoes over the wharf, the methodology drew attention to the risks of increased road traffic and ship movements in the harbour, as well as physical hazards to the public. By looking at the operations in terms of the three aspects — by process, by work-area and by activity — the chance of overlooking a particular hazard was minimised by keeping an open mind on the possible risk factors.

Event Grading

The OSH method is an example of risk assessment by estimating the severity level of possible consequences arising from a realised hazard. A more detailed classification into categories can be obtained by considering a wider range of effects, including:

- Harm to persons in terms of injury and illness (as in the OSH method);
- Damage to assets and property;
- The effect on the environment;
- The impact on the reputation of the organisation;
- The harm to the business of the organisation.

The Australian/New Zealand Risk Management Standard gives a useful listing of sources of information and provides examples of qualitative measures of risk and likelihood, which can then be used to develop a risk-level matrix. A number of similar matrices may be drawn up to fit the circumstances of an organisation. One such matrix of impacts is set out in Table 5.1, in which the effects of a realised hazard on various things and people are assessed qualitatively. Although this table was originally derived with a manufacturing or process facility in mind, the matrix can be applied to any engineering works. For a structure such as a major dam, for example, a class V ("catastrophic") hazard might be one which resulted in loss of life, permanent or long-term environ-

Table 5.1: Effects rating of a realised hazard (after Gillett[7], with modification)

Rating	People	Assets	Offsite	Reputation	Business
0 Insignificant	none	none	none	none	none
I Slight	minor injuries	slight <$5000	none	none	slight
II Significant	lost-time injuries	significant <$50 000	small not lasting	Limited (local news)	perceptible at unit level
III Major	some disabilities	major <$500 000	localised onsite impact	Regional news	affects whole enterprise
IV Severe	some fatalities	severe <$5 million	offsite impact	National news	shareholder concern
V Catastrophic	many fatalities	widespread >$5 million	major offsite impact	International news	pressure to halt business

mental damage or the destruction of heritage buildings and sites.

A likelihood rating may be set from experience of witnessing or hearing of the realised hazard, as illustrated in Table 5.2. For a facility that may last several years, the relative frequency might have units of events per year, and thus a "likely" event is one that is observed in a person's lifetime. For activities of shorter duration, such as a construction project, a correspondingly shorter time scale would be chosen (say events per week), and higher-frequency events would be looked at.

Table 5.2: Likelihood rating of a realised hazard (after Gillett[7] , with modification)

Rating	Remoteness	Experience	Relative frequency
A Negligible	Unlikely	Never heard of it	10^{-4}
B Low	Seldom	Heard of it	10^{-3}
C Moderate	Likely	Incident has happened	10^{-2}
D High	Almost certain	Happens several times elsewhere	10^{-1}
E Serious	Certain	Happens several times here	1

Some hazard-ranking schemes involve elaborate weighting of various factors that are believed to be significant in determining some kind of risk score. In reviewing the system employed by the Environmental Protection Agency of the United States to evaluate the risk of hazardous waste facilities, Haness and Warwick[8] note that small amounts of extra information can have a marked influence on the final score. There is a trap of adding a safety factor upon safety factor, with little or no consideration of the effect of cumulative errors. Such ultraconservative analyses are probably of little value. It is better to assess each factor separately within a coarse ranking, as in Table 5.1.

As with the OSH risk-rating method, the categories for impact and frequency may be combined to obtain an overall assessment of the danger of the realised hazard. The various scales in these tables are not linear; they approximate to a logarithmic scale, as indeed implied by the scale of relative frequency. Likewise, the scale of business impact in Table 5.1 varies from under $5000 for a level I risk to over $5 million for a level V risk. The Australian/New Zealand Risk Management Standard does not make this point clear.

The following Case Study 5.2 describes the use of risk analysis as a means of allocating resources to determine the most cost-effective way that a public utility could cope with failures and preserve the integrity of the network. In such a case, the risk need only be "measured" in comparative terms, and there is no necessity to evaluate risk levels on some absolute scale. Significant benefit can thus be obtained at relatively low cost.

Case Study 5.2 Risk Analysis of a Pump-Station Network
(Bermingham, 1999, *pers. comm.*; courtesy North Shore City Council and Peter MacKellar of Sinclair Knight Merz))

The Council required a risk analysis of all 84 wastewater pumping stations it owned and operated.

The study was based on the identification of failure mechanisms that resulted in dry weather overflows, the analysis of failures and the examination of various risk mitigation options. The study took a two-stage approach.

Initially a broad analysis of the 68 'local' stations identified the pumping stations which presented the highest risk.

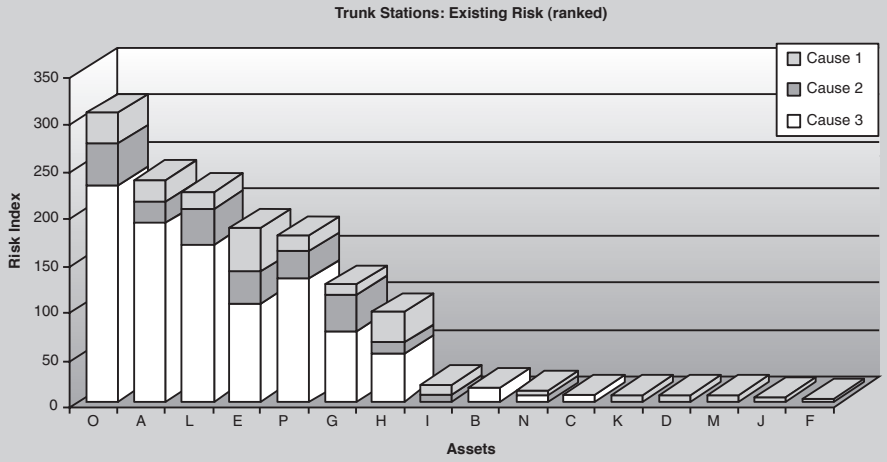
Detailed analysis of different failure scenarios at each of the 20 pumping stations identified as posing a high risk was then undertaken. The failure scenarios ranged from power failure, mechanical failure at the station, and rising main failure through to fire within a station. A risk model simulated the effect of each of the failures, taking into account existing contingencies within the system, such as site generators and emergency response measures.

Expressions were derived for the volume, duration, ecological impact, pubic health concerns and loss of public amenity, all of which result from an overflow. Risks were calculated for each failure scenario and summed to provide a total measure of risk for

each station.

A number of risk mitigation options were simulated and costed to assess the associated reduction in risk and their relative cost effectiveness. The results provided guidance to the Council to enable the development of long-term and cost-effective strategies to reduce the risk of dry weather overflows from the wastewater pumping stations. They also provided a means to refine and amend the Council's emergency planning procedures.

This project shows how a risk-based approach can facilitate policy in the allocation of resources, as well as identify the most cost effective mitigation options. As studies of this type are used essentially to allocate resources, risks need only be measured in comparative terms. This avoids the often-problematic steps of defining an absolute measure of risk. Highly valuable results can therefore be obtained at relatively low cost systematically improving either network or process integrity.



A number of risk-management options were evaluated and costed to assess the relative reduction in risk and their relative cost. The results providing guidance to the local authority to enable the development of long-term, cost-effective strategies to reduce the effect of dry weather overflows from their wastewater-pumping stations and provided a means of improving the Council's emergency-planning procedures.

Short-Cut Risk-Analysis Method (SCRAM)

A short-cut risk-analysis method, which Wells[9] has evocatively given the acronym "scram", was developed to provide a quick means of getting an estimate of the significance of an identified hazard in a Hazop review. A risk rating *RR* is obtained by summing the logarithms of parameters which reflects the frequency *F*, the severity *S* and the likelihood ϕ of mitigation by strategic or tactical means:

$$RR = \log F + \log S + \log \phi$$

Order-of-magnitude estimates are used for the frequency F, based on experience or generic data. The severity scale (as log S) may be taken directly from the risk rating in the first column of Table 5.1. (For example, a significant hazard, with a II rating, would be given a value of 2 for log S). The mitigation factor is often absent, as in a sudden dam failure. For a manufacturing or process facility, with an opportunity for intervention by an operator or a process-control system, log ϕ may be taken as -2. Wells[9] suggests that risk reduction is needed if the RR value is zero or greater.

There are a number of variants and developments of this method. Wood and Tweeddale[10] describe a risk-assessment study of the hazards associated with a range of industries in the Rosebank Peninsula, Auckland. A sample of ten installations was taken covering industries such as chemical manufacturing, light engineering and metalwork, foundry operations and general engineering contracting. Three impact scales were considered:

1. The impact to people expressed as fatalities, with injuries and nuisance defined arbitrarily as fractional fatalities;

2. The impact on property, on a scale of "houses destroyed";

3. The impact on the environment in terms of an arbitrary scale of toxicity and persistence.

Since there was incomplete records of event rates, a scale based on verbal descriptors was devised, ranging from a "very frequent" event, which was given a frequency of 0.5 per year, to a "barely credible" one of once in 100 000 years. The study provided a ranking of the industrial hazards and demonstrated that potential impacts to people living outside the industrial area would be limited to smoke nuisance from large fires and road accidents involving the movement of hazardous cargoes.

Except for certain high-hazard occupations, deaths in the workplace are uncommon in New Zealand, and those to the public from industrial activity are virtually unknown, Keey[11] has suggested a criterion based on the "numbers affected" by the realised hazard. In regard to the persons at risk, the criterion would be taken as the maximum number of people likely to be directly affected by the incident, whether in terms of physical personal harm or through disruption to normal activity for a stated minimum period (say 1 hour) or by psychological disturbance. The latter number reflects the concept of the United Kingdom Health and Safety Executive[12] in defining a "dangerous dose", the quantity of released energy or material that would cause severe distress to almost everyone in the incident under consideration. It would include the 6000 who were evacuated at the time of the Parnell fumes emergency. The risk rating then would then have units of the annual probable number of people affected by the particular realised hazard.

A measure of effects that reflects public perception of danger is difficult. One solution used by engineering consultants Kingston Morrison (now Sinclair Knight Merz) involves splitting an effect into its duration and its extent, which may be measured in area, volume or people affected (Bermingham 1999, *pers. comm.*). This approach was used to estimate the risks of extending the wastewater-treatment plant at Mangere, as described in Case Study 6.1 in Chapter 6. The method is essentially similar to that employed earlier by Wood and Tweeddale[10] in their analysis of impacts from industrial activity, in which the severity of the environmental impact was rated according to its long-term persistence as well as the physical damage that might ensue. There is no single measure of "effect".

These various short-cut methods yield a risk rating which is an index of the hazard potential. A number of these indices have some physical significance, being related to some averaged impact, and thus provides a conceptual indicator of the extent of possible danger. Care must be exercised in their interpretation because of the "soft" nature of the "data" that are used to obtain the rating. In the case of material-related hazards, risk indices based on more sophisticated algorithms have been developed based on process industry experience. These are reviewed briefly in the following section.

Risk Indices

Probably the most widely used risk index is that developed by the Dow Chemical Company in the United States. First devised in 1964 as a guide to the selection of fire-protection methods, the *Dow Fire and Explosion Index* has run through seven editions to 1994. Although devised for assessing onsite process-plant hazards, the index has been adopted to develop criteria to determine what operations are acceptable as predominant uses in industrial zones[3]. However, the detail needed for the method renders it unsuitable as a general-purpose tool for planning applications. It serves better as an inhouse means of comparing process options.

The method hinges on determining a *material factor MF* which reflects the inherent hazardousness of the principal substance being processed or stored. The calculation is done for each major process unit or storage facility on the assumption that there is a minimum inventory of about 2 tonnes of material. For lesser amounts of material, the Dow index would overstate the hazard potential. The material factor is modified by two penalty factors, one for *general process hazards* (F_1) that relates to items like material handling, drainage and spill control and another for *special process hazards* (F_2) for operation under intensive conditions such as temperature and pressures away from ambient, the use of rotating equipment, and the amount of unstable or flammable material involved. The fire and explosion index *FEI* is then calculated as

$$FEI = MF \times F_1 \times F_2$$

The *FEI* value is proportional to an exposure radius from which a damage factor is obtained. Various loss-control credit factors are suggested, based on the site's and plant's safety provisions: these enable estimates to be made of the maximum probable property damage and outage time from the given damage factor. Although the procedure is straightforward, the various parameters in the methodology involve numerous judgmental factors based on industrial experience which is unlikely to be universal.

There is a separate guide for chemical exposure.

The Mond Index was developed from the 1973 version of the Dow Index by the then Mond Division of ICI Ltd in the United Kingdom. It takes into account certain extra hazard aspects, with offsetting factors for preventive and protective features, as set out in the later editions of the Dow Index.

The instantaneous fractional annual loss (*IFAL*) is an index developed by the Insurance Technical Bureau primarily for insurance-assessment purposes. The method, which is described by the Bureau in their *IFAL p Factor Workbook*, is based on modifying a "p-factor", which is the equivalent of the material factor in the Dow index, by two parameters that relate respectively to standards of engineering (*e*) and of management (*m*), judged (presumably) on the basis of the insurance record:

$$IFAL = p \times e \times m$$

In well-engineered and well-managed plants, both *e* and *m* are unity, so the *IFAL* and the *p* factors are identical in this situation.

Event-Tree and Fault-Tree Analysis

Event and fault trees are two kinds of logic diagrams that are useful in tracing fault and mishap pathways leading to unwanted outcomes (accidents). Event trees were first developed in the aerospace and nuclear industries as a means of following the progression of some primary incident through a series of binary branches representing success or failure of safety features or the presence or absence of some physical condition. Thus an event tree traces all the possible outcomes of the initiating event.

A fault tree, on the other hand, starts with the top event and traces all the branches from the crown to the root causes of that particular outcome.

Event trees are sometimes used to check whether all the branches have been incorporated in a fault tree, for which it is easier to overlook a pathway to failure.

Fault trees are commonly employed in quantitative risk analysis to estimate the remoteness of a perceived outcome, and qualitatively to demonstrate safety features and mitigating circumstances that reduce the likelihood of the outcome being witnessed.

Event-tree analysis. Figure 5.1 illustrates a simple event tree for a car skid when the driver loses control: an accident may or may not result.

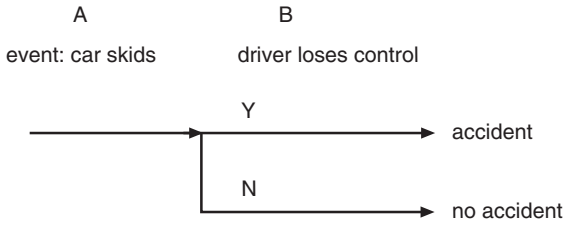


Figure 5.1: Event tree for a car skid

So the probability of there being no accident *P(C)* is given by

$$P(C) = P(A)\Sigma\overline{P}(B)$$

where $\overline{P}(B)$ is the complimentary probability of seeing event *B* and equal to 1 - *P(B)*.

Event trees are particularly useful in tracing the escalation of an emergency into increasingly more dangerous situations, as Figure 5.2 demonstrates.

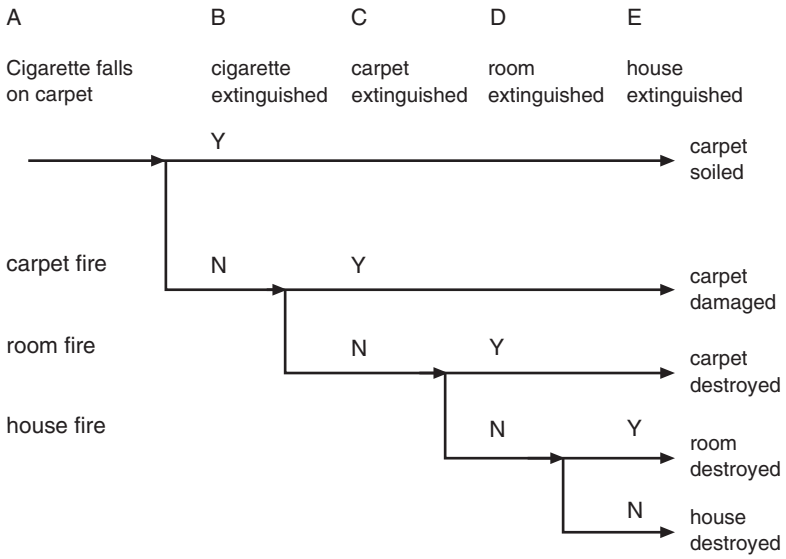


Figure 5.2: Event tree for a house fire caused by a burning cigarette

Another example of the use of an event tree in risk assessment is the study[13] by Sydney Water of the stability of a dam under both earthquake and rapid drawdown conditions. The authors considered the case when a major slip might have occurred on the upstream shoulder of the dam without causing an immediate breach. Would there be any remedial response or not? The analysis involved considerations such as:

- what options could be taken to prevent the failure slip from progressing to a total breach;
- what was the likelihood of these actions being successful;
- what would be the response time at various stages in a developing breach?

These factors would depend upon the magnitude of the earthquake and its effect on the infrastructure in the area affected.

An example of this approach has been given by Turner and Shuster[14]. As shown in Figure 5.3, an event tree is developed to choose a method to secure an unstable slope, whether to install a drainage system or flatten the slope. The consequence and cost of each outcome are separately assessed. The consequence of each pathway is measured in monetary terms as a relative loss. Conceptually, the figures might represent thousands of dollars. The expected cost is the sum of the various products of path probability and loss. The event tree, in this case, suggests that there may be a slight advantage in installing a drain compared with flattening the slope, but some treatment of the slope would be worthwhile.

Fault-tree analysis. The construction of a fault tree is also straightforward, being based on the logic rules for the combinations of events, but there are a number of pitfalls for the unwary. If two events happen together, the events are said to pass through an AND gate. The probability of seeing this occur, $P(T)$ is less than the probability of seeing either of the primary events A and B:

$$P(T) = P(A) \bullet P(B)$$

On the other hand, if two alternative events can give rise to a secondary event, the primary events are said to pass through an OR gate, and the likelihood of seeing the top event is greater than either of the two primary events:

$$P(T) = P(A) + P(B) - P(A) \bullet P(B)$$

where the probability $P(A) \bullet P(B)$ represents the chance that the two events A and B may happen together. Whenever the incidence of these primary events is infrequent, the likelihood of them happening simultaneously may be ignored.

A fault tree is a logic diagram and is not a representation of a flow of material or current as in a process flowsheet or circuit diagram. Whenever a component

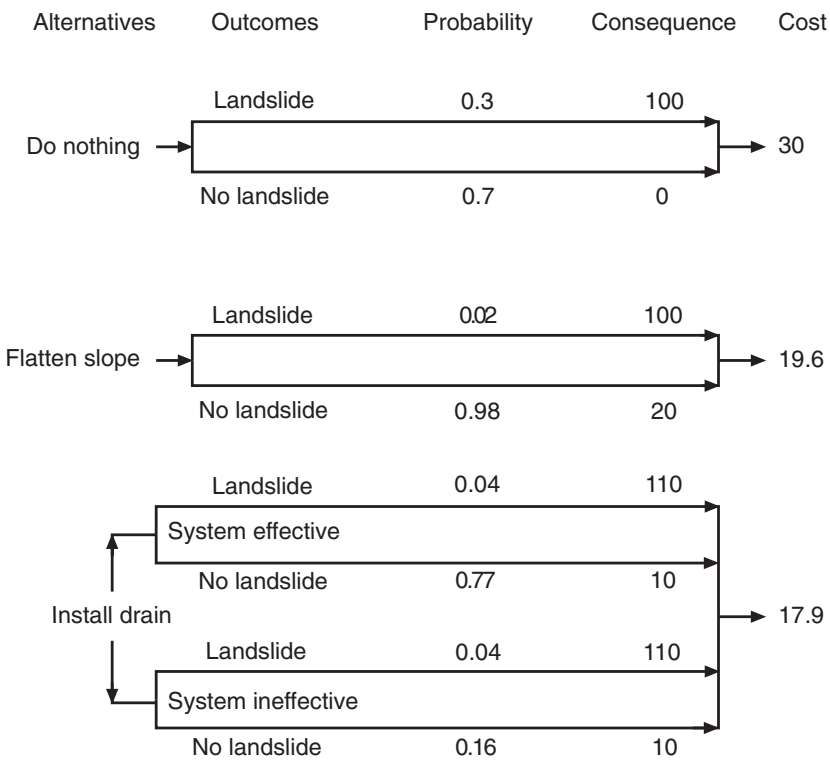


Figure 5.3: Use of an event tree to estimate a geotechnical risk (Turner and Schuster[14], reproduced in BRANZ Study Report No. 83, 1999, with modification)

has more than one operational state, there needs to be an initial condition specified for that component. This is treated as a conditional probability through an AND gate.

The object of a fault-tree analysis is the determination of the minimum number of basic or undeveloped faults and mishaps that in combination will give rise to a particular outcome. A *minimum cut set* of events is one that does not contain another cut set. The complete number of minimum cut sets represents the principal failure modes for the top event. Failure to determine these sequences, with the inclusion of duplicated pathways, can lead to grossly false and misleading estimates of the "top-event" rate.

The reduction of a fault tree to the minimum sequence of events may be done by Boolean algebra or some other systematic method. Fussell's algorithm[15] is particularly attractive for this purpose as the methodology can be adapted to a spreadsheet representation for hand or computer-aided evaluation. The method is described by Lees[16] and is reproduced in Appendix A with a worked example.

A simplified fault tree for estimating the probability of a turnover of a railway train at a sharp bend is illustrated in Figure 5.4. The numerical values of human reliability have been based on modified estimates from industrial psychologists and are included solely for illustrative purposes; the relative magnitudes are more significant than the absolute values. The fault tree demonstrates that the most significant prime cause derives from the train driver entering the curve too fast by not braking in time, a conclusion not known until the full fault tree had been developed.

Figure 5.4 also shows that a fault tree contains a mix of AND and OR gates, in some cases a considerable number. Extensive fault-tree development demands significant resources in time and data research. In most engineering applications, such a technique would only be used to investigate specific issues of major concern that have been identified by less rigorous methods.

The various input probabilities are not single-valued, but some kind of mean within a range. The best failure data record appropriate range variables. (The much-maligned but seminal Rasmussen Report (AEC 1975), for example, gives

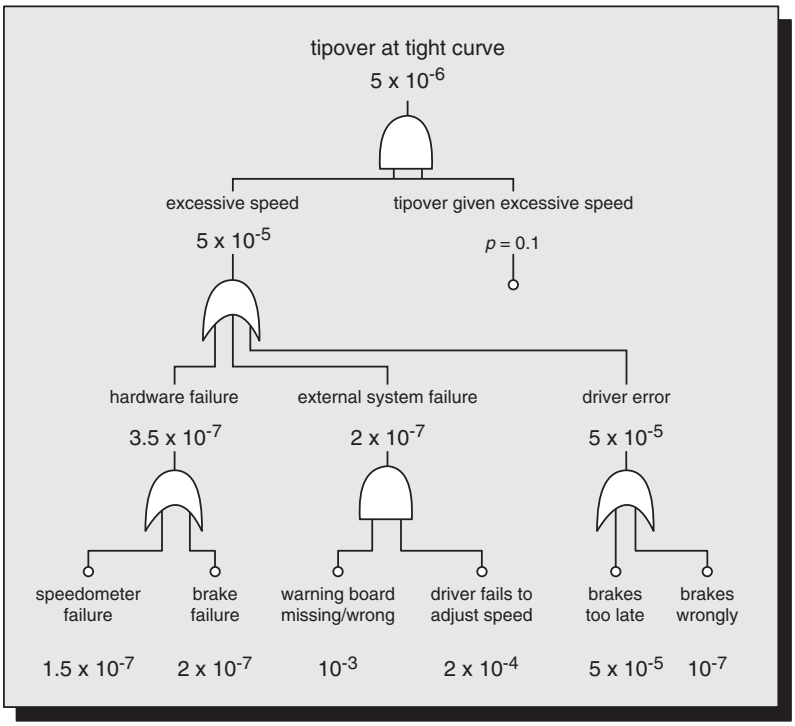


Figure 5.4: Simplified fault tree for the turnover of a train at a sharp bend (After Elms 1998, pers. comm., with modification). Probability values are indicative and do not necessarily refer to actual practice.

median values and the failure-rate ranges for a large number of process components used in the nuclear power industry). Keey and Smith[17] note the variance (or range) changes as events propagate into higher-order incidents. The outputs from an OR gate shrink in range but increase in frequency: those from an AND gate spread in range but become more remote. The effect in a large fault tree thus depends upon its branching network, and some uncertain input events may have little impact on the outcome. The price we pay for remoteness is uncertainty.

Databases for use in fault trees are of two kinds: either relating to incidents or to equipment reliability. For scoping studies, there are some data in the public domain (e.g. Lees[16], Smith[18]). Large organisations will normally have aggregated other data from their own experience and maintenance records. The investment of effort in creating and updating a useful database is substantial, and this has led to the development of large databanks by national authorities. The United Kingdom's Safety and Reliability Directorate runs the National Centre for Systems Reliability and Systems Reliability Service. Originally the databank was based on the use of mainframe computers, and contained databases for generic reliability, events, accidents, human reliability and maloperation, but now has been modified to be handled on desktop machines. An incident database known as FACTS is operated by the Netherlands Safety Organisation, TNO, with data gleaned from the literature, industry and inspectorates in various countries. There is also commercial software containing menus of failure rates and failure modes suitable for use on desktop computers.

A number of companies offer software for the generation of fault trees themselves. There have also been attempts to enhance informal methods of drawing up the trees. Khan and Hunt[19], for example, describe a computer-aided method of developing fault trees, FAULTFINDER, which can be integrated into process-design software to generate fault-propagation pathways from information given in a process flowsheet.

Fault-tree analyses were first used in New Zealand by A D Little Inc. in the safety assessment of a proposed nationwide bulk LPG distribution and storage network for Liquigas Ltd, and independently by TNO for the former Liquid Fuels Trust Board[20]. More recently these techniques have been used to investigate the safety of rail operations for Tranz Rail Ltd[21]. The methodology is also suitable for looking at the behaviour of smaller systems. Powell[22] has used fault-tree methods for determining the explosion risk of valve-vented, domestic water-storage heaters.

Enhanced Reliability

In a number of instances, a failure of an engineering component or a loss of engineering services can lead to a disaster or gross inconvenience. In such

cases, a very high degree of reliability is demanded for security. Informally, we regard the absence of a prior failure as providing some assurance that there will not be a failure in the future. This experience, however, only provides a limited assurance. For instance, if an engineering component has not failed in the first five years of its life, we can only say that the likely failure rate is no greater than once in five years (the component may fail tomorrow!). With a failure rate of this magnitude, the chance of failure in the next year is still significant (it is 9.5%), and thus there is no great confidence in the component's future reliability over this period.

It is possible to enhance the reliability of an engineering system by providing redundancy. The redundancy may be active, in which case all subsytems in use are in parallel, and the system as a whole only fails when a given number or all of the components fail. Suppose our engineering component was duplicated to provide active redundancy. If there had been no failures in the first five years, then the chance of failure in the next has now been reduced to 0.9%, a tenfold reduction. Active redundancy may be partial. An aircraft that can fly on two of its four engines is an example of this. Alternatively, the redundancy may be passive, and a standby item is switched into service only when the primary unit has failed. While this is a useful arrangement in an industrial location where the failed unit can be immediately repaired and replaced, the benefit of standby is only achieved if the switchover is reliable and the auxiliary unit will work when called upon.

A recent example of standby failure has been cited by the *Chemical Engineer*[23]. The supply of electricity to the fuel-cycle area of the Dunreay nuclear plant in Scotland was cut off when an excavator hit power lines. The site's emergency diesel generators did not start up, causing the ventilation system to shut down. Fortunately, the system that monitored the discharges from the plant was powered by a separate battery-backed supply, so that no abnormal discharge from the plant was thought to have taken place. (One may note, in passing, that the prime cause of this accident was loss of management control in allowing the digger to strike the cables!)

Thus reliance on standby systems can sometimes be misplaced. The expected reliability will only be achieved whenever the standby is of equal performance as the primary unit, implying regular testing to ensure that it is operable when called upon, and the switchover at the time of the primary failure is flawless. There may be a temptation to rely on systems of lesser performance for backup equipment on the assumption that they will be rarely, if ever needed, and the diminished performance can be tolerated over the repair period.

Sensors that are reliable at detecting fault conditions may give spurious trip signals or have "fail-safe" faults that cause disruptions (such as premature bursting-disk failures protecting high-pressure vessels). The reliability for the given

purpose may be called the *responsibility* of the system. A way of achieving enhanced responsibility is the use of voting systems. Voting arrangements enable false signals to be discarded on the assumption that the reading of the majority is correct.

One should be wary of claims of very high reliability unless the system has been carefully designed. A system of apparently very high integrity can be compromised if all of its supposedly independent control features can be subject to a common-mode fault, such as a power failure. There are practical limits. Kletz[24] cites the example of a protective system with a fractional deadtime of 0.01 (to take account of the time needed to test the system for continuing operability). If the system were triplicated, the fractional deadtime would apparently be reduced to 10^{-6} if the testing were staggered. This implies that the deadtime of the whole system is less than one minute per year which hardly seems possible if manual checking and inspection are demanded.

Hazard Warnings

Fault-tree analyses were developed in the aerospace and nuclear-power industries, where their effectiveness came under criticism after a period of use. Bryan[25] noted that the traditional method of assigning historical probabilities to events had led to overly optimistic conclusions in the light of unexpected test and operational failures. Some of these had been considered to be incredible previously, while others had been overlooked in the initial analysis. Moreover, fault-tree methods are based on classifying conditions into discrete states of success or failure, whereas normally operational conditions are more likely to reflect a range of partial success. Thus, fault trees do not serve as infallible guides to the remoteness of a hazard, despite their apparent mathematical rigour. Their power lies in comparing alternative strategies, checking safety concepts and discovering weak points in a system's reliability.

A fault tree illustrates that an accident arises whenever some kind of mishap can escalate into a more serious incident should there be a failure of some blocking measure or mitigating circumstance. In most cases, some or all of these features will be present to stop the accident happening. The primary mishap thus acts as a warning that something more serious might have occurred. Some industries regularly investigate all incidents regardless of size to determine whether further safety features or procedures are needed.

More serious accidents are thus less frequently witnessed than those of lesser consequence. This observation has often been demonstrated by drawing an accident triangle: for every fatal accident there are some lost-time injury accidents, more minor injury accidents, and so on, as shown in Figure 5.5. The seemingly inconsequential mishaps serve as warnings. Monitor these, and one has some idea of the remoteness of more dangerous accidents, but also an in-

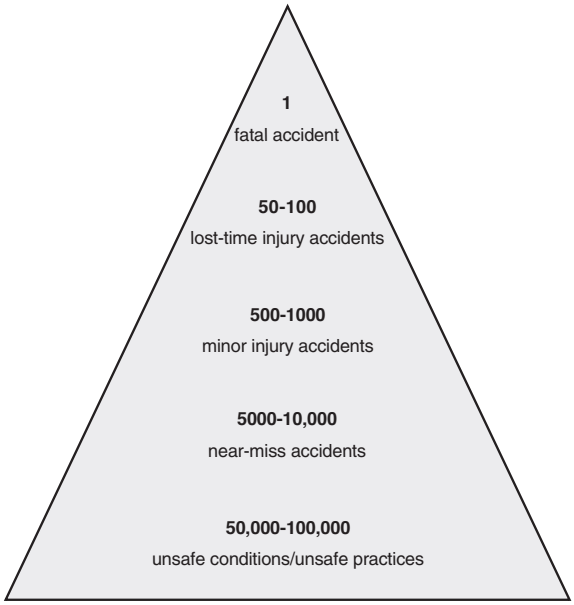


Figure 5.5: The triangle of industrial accidents. (The numbers are indicative and vary with the occupation).

sight into the means of preventing them happening. Likewise, an indicator of changing levels of safety on a manufacturing facility would be a monthly audit of things such as: the number of leaking seals and flanges, the number of instruments out of working order and being repaired, and general equipment and plant tidiness.

The probability of seeing the top event of a fault tree, $P(T)$, is much less than that, $P(W)$, for seeing a warning by a factor p:

$$P(T) = p \bullet P(W)$$

In an illustrative example, Lees[16] considers the case where the top-event frequency is 0.001 yr^{-1} and warnings are expected to appear at two-yearly intervals. (The p factor is 0.002). Over a ten-year period, the probability of seeing the top event is 1%, but the probability than there will be a failure of witnessing two hazard warnings in that time is only 0.04%. There is thus a useful degree of warning. If more warnings take place than expected, then the system can be examined to determine whether there are any previously unsuspected weaknesses. If there are fewer warnings, then the system may be safer than originally thought. This is a very powerful tool that is not limited to plant-related risks. The concept of hazard warnings is generic, and can be applied to all kinds of safety and health issues.

Fault trees can be recast as hazard-warning trees to determine the various levels

of safeguards fitted to a system and the possible mitigating circumstances which might be present. The presence of multiple attenuation factors (yielding a very small p factor) is perhaps more significant in the assurance of safety than a very low calculated value of the top-event frequency itself. For example, an above-ground storage tank for liquefied hydrocarbons under pressure will only be torn apart in a boiling-liquid expanding-vapour explosion ("bleve") when a leak is not stemmed and the accumulated liquid catches fire under the tank, the flames play on the vessel for many minutes, the water-deluge system fails, and the combined efforts of staff and the fire-brigade are unable to cope with the blaze. Notwithstanding the high hazard potential of hydrocarbon liquids held under pressure, the storage is regarded as "safe" because of the multiple safeguards in preventing the final outbreak.

Evaluation of Consequences

In some cases, the consequences of a hazard being realised are determinate: the outcome is known. This is the situation with mechanical breakdowns of equipment which do not trigger secondary failures. In other instances, when there is a release of hazardous material or energy, the impacts may be far-reaching and the effects are more indeterminate.

In the case of geotechnical hazards, Finlay et al.[26] summarise the vulnerability of persons in open spaces, vehicle and in buildings from historical data based on experience in Hong Kong with landslips. Some values are reproduced in Table 5.3.

In general, the consequence of an accident is related to the generated force or released quantity of excess material or energy. Since only a small amount may have a perceptible effect on a person or property, and a full impact may require a considerable amount, the likelihood of a given effect is normally given in probabilistic terms. One measure that is sometimes used is the *probit* (prob-

Table 5.3: Vulnerability ranges to persons from landslide debris. Probability of death from the given event.

Case	Range in Data	Recommended Value	Effects
If struck by rockfall	0.1-0.7	0.5	May be injured
If buried by debris	0.8-1.0	1.0	Death by asphyxia
If not buried	0.1-0.5	0.1	High chance of survival
If vehicle is damaged only	0-0.3	0.3	High chance of survival
If building collapses	0.9-1.0	1.0	Death is almost certain
If debris strikes building only	0-0.1	0.05	Virtually no danger

ability unit). It is a random variable with a mean of 5 and variance 1. A probability of 95% corresponds to a probit of 6.64. A transformation of probability percentages to probits is found in a number of texts (e.g. Lees[16]). The probit variable Y is a linear function of a parameter X, which is a measure of the intensity of the causative factor producing the harm:

$$Y = k_1 + k_2 X$$

where k_1 and k_2 are constants that depend upon the specified level of harm (such as the extent of burns to an onlooker from a fierce fire). Eisenberg et al.[27] give some values for these constants for personal injury and structural damage. The advantage of using the probit is that this expression for harm is linear, and reduces the difficulty of assessing extreme events with the underlying sigmoid dose-effect curve.

For an explosion, the parameter X is taken as the peak local overpressure. In the case of fires, X is interpreted as a thermal dose defined by $I^{4/3}t$, where I is the local intensity of radiation from the fire and t is the exposure time. With a release of a toxic gas, X is also taken to be the integral dose $\int c^n \, dt$, where c is the concentration of the toxic substance in the gas and n is an exponent that normally lies between 1 and 3.

The spread of gases is usually calculated on the basis of diffusion theory, with the "diffusion" or dispersion coefficients obtained from empirical experience under particular meteorological conditions. While such calculations are reliable under the specified conditions over flat ground, they may lead to uncertain or inaccurate predictions in actual situations of uneven terrain and in the presence of tall obstacles such as buildings and other structures. One commonly used model in Australia and New Zealand is AUSPLUME, which is based on the premise that cross-sections through elevated plumes from point sources of a substance have a Gaussian or normal distribution of concentration. The model contains a subroutine to allow for the influence of wakes from buildings on the dispersion from a stack. There are also suggestions to correct for a change in terrain elevation. Details may be found in the Victorian EPA Publication, number 264.

There are commercial software packages, such as WHAZAM-II and SAFETI, which incorporate consequence calculations.

The extension of these methods to evaluate environmental risks poses formidable difficulties in modelling, particularly in assessing the long-term impacts of a number of releases which individually may be considered to be minor or negligible[28,29]. Such modelling requires knowledge of the history of the releases, and the mechanisms of dispersion and accumulation at sensitive sites, as well as ecotoxicity data.

There are also problems in assessing effects at very low doses. Cothern et al.[30] note that disparities of several orders of magnitude are found in trying to determine the risk from the presence of extremely small concentrations of trichloroethylene (TCE) in groundwater by extrapolating data for the effect at much higher concentrations, depending on the method used.

Clearly any extrapolation of data demands the use of an appropriate model of the effect mechanism, rather than relying on an arbitrary extension of any correlation beyond its tested range. The choice of such a model may be a matter of contention.

Despite many years of research, the effect of low doses of ionising radiation, for example, is still the subject of much debate. A somewhat similar argument has arisen more recently around the effects of electromagnetic radiation from cell-phone towers and high-voltage transmission lines. Current safety standards are based on the thermal effects of this radiation, with significant derating from these levels to give a safety margin, but there are still worries expressed from laboratory studies that athermal effects to body cells may be present also.

Case Study 5.3 Risk Analysis of a Wastewater Treatment Plant
(Bermingham, 1999, *pers. comm.*; courtesy Anchor Products Ltd)

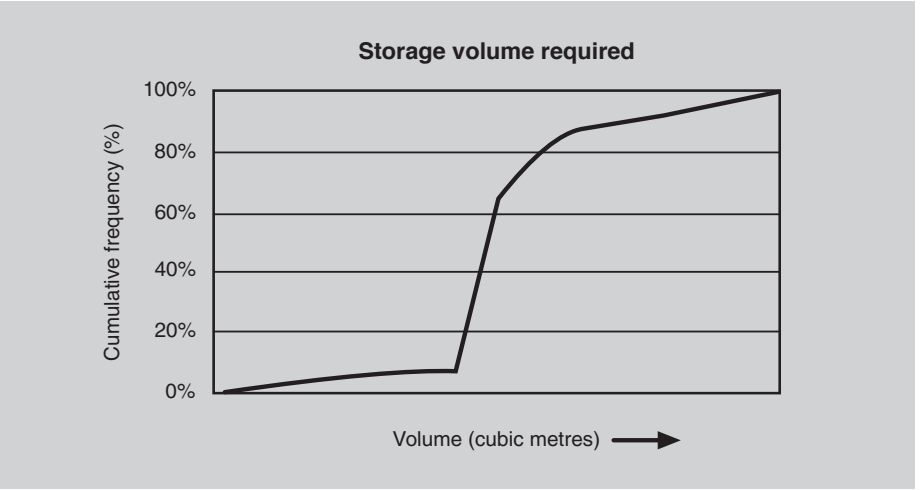
The plant is located at Te Rapa, near Hamilton, and the cultural and environmental sensitivity of the surrounding environment together with the technically advanced nature of the process being employed led to uncertainty over the response of the site's waste treatment plant under certain conditions. The site owner wished to gain a better understanding of the plant's behaviour under such conditions and, if necessary, implement design changes.

As a number of different incidents were possible, a "bottom-up" approach was adopted for the analysis. Additional probability simulations were employed to analyse the loading on specific elements of the design.

The main elements of the plant were investigated in turn to identify all credible fault conditions. For each one, the effect of these upsets on the process effluent was recorded together with the anticipated likelihood of failure. The consequential effects on the environment and on site production were classified against a previously defined scale.

As the results of the initial analysis demonstrated that the stormwater basin would become overloaded under some conditions, a separate probability-based simulation was carried out. This demonstrated that the design may not be able to act as an effective contingency volume under some fault conditions. The simulation was therefore extended to identify the optimum volume for separate contingency storage.

The risk analysis demonstrated that the fitting of the additional storage tank would lead to a five- to six-fold lowering of environmental risk and a significant reduction in resources required to cover for process fault and high load incidents.



References

1 Hynes, M and Vanmarke, E (1976): "Reliability of embankment performance prediction", in *Proc. ASCE Engng Mechanic Div. Conf.*, Waterloo, Ontario, Univ. of Waterloo Press [reported by Pidgeon et al.(1992)]

2 Dunster, H J and Vinck, W (1979): "The assessment of risk - its value and limitations", *Eur. Nuclear Conf. Foratom VII Cong*. Hamburg, 162-166, Vulkan-Verlag, Essen. [reported by Crossland et al. (1992)].

3 Palmer, E R (1990): "Town planning criteria for operations with hazardous chemicals", *Proc. Annual Conf. 3*, IPENZ Wellington, II, 73-84.

4 Bond, J (1996): "*The Hazards of Life and All That*", Inst. Physics, Bristol.

5 Keey, R B (1987): "*Reliability in the Process Industries*", IPENZ, Wellington.

6 Sherwin, D J and Lees, F P (1980). "An investigation of the application of failure data analysis to decision-making in maintenance of process plant", *Proc. IMechE. 194*, 301, 308.

7 Gillett, J (1985)"Rapid ranking of hazards", *Proc. Eng*., February 1985.

8 Haness, S J and Warwick, J J (1991): "Evaluating the hazard ranking system", *J. Environ. Management, 32*, 165-176.

9 Wells, G (1996):"*Hazard Identification and Risk Assessment*" IChemE, Rugby, UK

10 Wood, S and Tweeddale, H M (1990): "Rosebank Peninsula risk assessment study - A review of safety and risks in an Auckland industrial area", *Proc. Annual Conf.* IPENZ Auckland, II, 51-61.

11 Keey, R B (1991): "A rapid hazard-assessment method for smaller-scale industries", *Proc. Safety & Environ. Protection*, 69(B2), 85-89.

12 Health and Safety Commission (1991): "*Major Hazard Aspects of the Transport of Dangerous Substances*", HMSO, London.

13 Landon-Jones, I, Wellington, N B and Bell, G (1995): "Risk assessment of Prospect Dam", *IPENZ Proc. Techn. Groups* 21/1 (LD), 55.

14 Turner, K A and Shuster , R L (1996). "Landslides: investigation and mitigation", *Trans. Res. Board Special Pub. Rep. 247*, reported in BRANZ Study Report No. 83, 1999.

15 Fussell. J B (1976): "Fault tree analysis: concepts and techniques", in Henley, E J and Lynn, J W (eds) "*Generic Techniques in Systems Reliability*", p 135, Noordhoff, Leyden.l

16 Lees, F P (1996): "*Loss Prevention in the Process Industries*", 2nd edn, Butterworth-Heinemann, London.

17 Keey, R B and Smith C H, (1984). "The propagation of uncertainties in failure events", *Reliab. Eng., 10*, 105-111.

18 Smith, D J (1993): "*Reliability Maintainability and Risk*", 4th edn, Butterworth-Heinemann, Oxford.

19 Khan, A R and Hunt, A (1989): "The propagation of faults in process plants: integration of fault propagation technology into computer-aided design", *IChemE Symp. Ser. No. 114*, 35-43.

20 Liquid Fuels Trust Board (1984): *"Risk Assessment of Future LPG Facilities in New Zealand"*, Rep. No. LF 5006, LFTB, Wellington.

21 Peet, W and Ryan, R (1998): "Risk management in a network operation: understanding complex systems", in Elms D G (ed.) "Integrated *Risk Management*", CAE, Christchurch.

22 Powell, L (1995): *"Explosion risk analysis for valve-vented storage water heater*s", BE (Chem.& Proc.) Rep., Univ. Canterbury, Christchurch.

23 Chemical Engineer, The (1998): "Power-cut hits Dounreay", 14 May, p 5.

24 Kletz, T A (1992). "*Hazop and Hazan*", 4th edn., IChemE, Rugby, UK.

25 Bryan, J L (1976): "The determination of behavior responses exhibited in fire situations", *J. Fire Flammability, 7, 319.*

26 Findlay, P J, Mostyn, G R and Fell, R (1997): *"Vulnerability to Landsliding"*, reported by Riddolls and Grocott Ltd (1999).

27 Eisenberg, N A, Lynch, C J and Breeding, R J (1975): "Vulnerability Model:

A Simulation System for Assessing Damage from Marine Spills", *Rep. CG-D-136-75, Enviro Control Inc, Rockville MD.*

28 Zach, L S and Keey, R B (1995): "Towards a methodology for environmental risk analysis", in Melchers, R E and Stewart, M G (eds) "*Integrated Risk Management*", 235-242, Balkema, Rotterdam.

29 Zach, L S and Keey, R B (1998): "Risk analysis of chemical contaminants in the environment: estimating the long-term consequences from frequent low-level accidents", *Proc. Conf. Environ. Strategies for 21st Century*, Singapore

30 Cothern, C R , Coniglo, W A and Marcus, W L (1986): "Estimating risk to human health", *Environ. Sci. Technol., 20(2), 111-116.*

31 Boyes, W J (1998). *"Risk Assessment for a Port Proposed at Marsden Point by Northland Port Corporation"*, BE (Chem and Process) Rep., University of Canterbury, Christchurch.

Data collection

6 Risk Evaluation

Risk evaluation is concerned with deciding whether a risk is tolerable or not. It is the next step of a full risk assessment (see Figure 2.3). The evaluation is used to determine policies for managing the identified hazards by evaluating and comparing levels of risk against predetermined standards, risk-target levels or other criteria of safety. These decisions hinge on judgements regarding the acceptability of risk. Strictly, no level of additional risk is acceptable, and often those who make such judgments do not face the imposed risks directly. Rather than speak of "acceptable risk" we talk of tolerable risk, the risk that can be borne in the meantime because of collateral benefits until the time we can do something better. A starting point for the search for tolerable risk levels has been the analysis of existing risks that society faces in various ways.

Subjective judgements, whether by engineers or others, are a major component of any risk assessment. If such judgements are faulty, then risk-management efforts are likely to be misdirected. An American study[1] in which respondents of various backgrounds were asked to rank thirty different kinds of hazards produced a wide range of viewpoints. A significant factor in making a judgement was the perceived potential for disaster rather than a particular risk posed. The use of quantitative methods of estimating both the remoteness of an identified hazard and the potential consequence should it be realised provides a basis for making a judgement with the minimum of subjectivity.

Many authorities, including the Australian/New Zealand Standard, consider risk assessment to include both the analysis and evaluation of risks. This chapter is concerned with the latter aspects, such as the tolerability of identified risks as a basis for the selection of options and defining risk-management policies.

A major risk assessment is expensive, costing several hundreds of thousands of dollars, and in some instances the cost can run into millions. It is not an undertaking entered into lightly. In almost every case, it is worthwhile to do a preliminary scoping and pilot study. This prior work is analogous to commissioning sketch plans or flowsheets before deciding to proceed to a detailed design and full working drawings. In some cases, this initial study could provide enough information for a risk-management decision without the need for a further, more detailed assessment.

Accepted and Imposed Risks

It is often claimed that people perceive a risk to be less serious if it has been accepted voluntarily rather than imposed. However, the correlation between

voluntariness and personal safety is only moderate. There are instances of involuntary risks that involve threats to personal safety, as in wartime, while it is debatable whether workplace hazards represent voluntary or involuntary risks. Voluntariness has to do with whether you blame yourself or others[2]. If the cause of an accident is human, we tend to attribute blame in proportion to the various agents. This process is seen in its most ritualised form in public inquiries and court proceedings that follow major incidents.

If we are already ill-disposed towards an agent because of perceived authority to control events which have been unilaterally imposed on us, then much stronger blame is attributed in the case of an accident than if we had willingly been involved in the decision-making in the first place. This reaction illustrates that a feature in distinguishing imposed and voluntary risks is the sense of personal control whenever risks are willingly undertaken. We believe, perhaps mistakenly, that we are now masters of our fate and not potential helpless victims of the rashness or callousness of others.

Individual and Societal Risks

Risks can be viewed in two ways: as threats to one's person, or threats to the wider community. These risks are rarely the same, and both aspects must be assessed. A person may be engaged in a hazardous activity at work which affects no-one else. The risk to society from this activity may be negligible compared with the other hazards of life, and indeed may bring societal benefits, but from the individual's viewpoint the hazard is far from slight. Conversely, a public health risk may be community-wide, resulting in significant healthcare and other costs, but the threat to any one individual could be very small indeed. Other examples include accidents involved many simultaneous deaths such as aircraft crashes.

Society is averse to the trauma of multiple-fatality accidents (often triggering public inquiries to determine cause) even though the individual risk might be shown to have been small. There is normally a call to make "things safer". The response of the Department of Conservation to the collapse of a viewing platform at Cave Creek, with its tragic loss of young lives, has been a thorough examination of facilities in the conservation estate, with the strengthening or withdrawal of structures not meeting safety standards. There is pressure to "remove accident backspots", despite evidence that improved roadworks may, in most cases, only have a minor effect on accident rates. Sabey and Taylor [3] report that the United Kingdom's Transport and Road Research Laboratory had found that in 65% of all accidents the road-user solely contributed to the accident, while a further 24% could be attributed to both the user and the road environment.

An individual risk may be defined as the annual probability of harm (injury or

death) to a given person in a particular place from a specified incident. This risk is the probability $P(C|F)$ of a particular consequence C following a failure or accident F, and the vulnerability $P(V|C)$ of a particular person given that outcome:

$$P = P(C \mid F) \sum P(V \mid C)$$

The vulnerability is likely to vary over a range of values for a particular consequence, as noted in the previous chapter for far-reaching effects.

The societal or group risk is the annual probability that a specified number of persons or more will be harmed to a given extent from a particular incident. Frequently, societal risks are displayed on terms of risk profiles, which are plots of probable incident frequency against the outcome (normally measured as fatalities per event).

Farmer[4] has plotted the annual frequency of events resulting in death from both natural and humanly-caused events to illustrate that, as risks becomes more severe in their consequence, so they become less common. These risk profiles of societal risk are reproduced in Figure 6.1. He noted that, while severe natural events may kill many thousands in a single event, even the largest of industrial accidents would be unlikely to kill more than a thousand. However, the differences in slopes, he added, might be due to limitations of data. Further, he remarked that it was difficult to ascribe a weight to a predicted event causing say 10 000 casualties at an estimated probability of 1 in 10 000 per year, which is not the same as a probable casualty rate of 1 per year for a relatively common accident! Other authorities have been less cautious. The Rasmussen report confidently predicted that accidents to nuclear-power stations involving 1000 or more deaths (based on a group of 100 reactors) was equivalent to the risk of a meteor striking a major city in the United States at an annual probability of 1 in a million.

Risk Criteria

Early attempts to derive criteria for the acceptability of risks tried to assess risk levels that society appeared to tolerate in everyday living. Rothchild[5] set an acceptable risk level as 1 in 7500 per year of exposure based on the number of car accidents in the United Kingdom in 1974. In the Netherlands, a waterways authority, Provincial Waterstaat Groningen[6], drew up criteria from earlier Dutch experience with flooding of low-lying land when sea-dykes were breached in a severe North Sea storm. A single fatality once every hundred years was considered to be on the borderline of acceptability (a hundred years being of order of a human lifespan), while incidents involving more than 1000 simultaneous deaths were deemed to be unacceptable. The scale of impacts was also related to a qualitative one for environmental damage, ranging from a local impact from

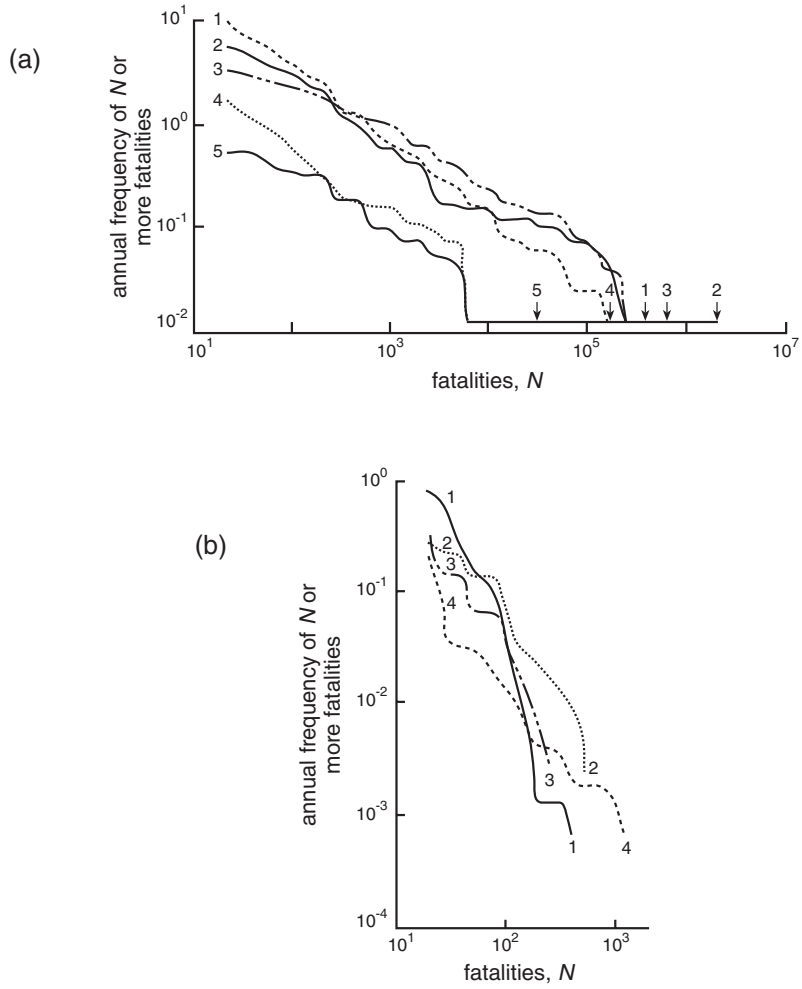


Figure 6.1: Risk profiles for (a) multiple-fatality accidents occurring worldwide from natural causes and (b) extrapolation of data on accidents occurring within the British Isles. (After Farmer[4])

the use of pesticides to a major disaster rendering a wide area unfit for human habitation for a long time (such as the impact arising from a major nuclear radiation release).

Earlier, the Delta Act of the Netherlands had prescribed that the water defences should be sufficient to withstand flooding of the "heart of Holland" with a failure probability of 1 in 10 000 per year. The Dutch Parliament set an individual fatality risk criterion of 10^{-5} (1 in 100 000) per year for existing risks involuntarily imposed on the basis that no risk of human origin should increase the individual risk of a young person, dying of natural causes, by more than 10

percent. For 12 to 16-year old youths, this health risk was estimated to be 10^{-4} (1 in 10 000) per year. With new projects, the limit was set one order lower, at 1% of the risk from natural causes (VROM 1985).

Farmer's curves have been used as a basis for risk-level bands of acceptability. The United Kingdom's Health and Safety Commission[7] has produced limits for intolerable societal risk in a report on the major hazard aspects of the transport of dangerous materials. An upper limit of "local tolerability" was based on the assessed risks from petrochemical facilities to the surrounding population on Canvey island in the Thames estuary when a risk of 1 in 500 years from an accident involving 500 deaths was considered "just tolerable" (Figure 6.2). The lower limit, representing risks that were deemed "negligible", was set at three orders of magnitude lower. A third line, one order below the upper line, is called the local-scrutiny line, and represents the bound for the particular neighbourhood of the associated road, rail or marine transport routes. The region between the upper and lower bands represents risks that are subject to improvement according to the principle that they should be "as low as reasonably practicable" (ALARP).

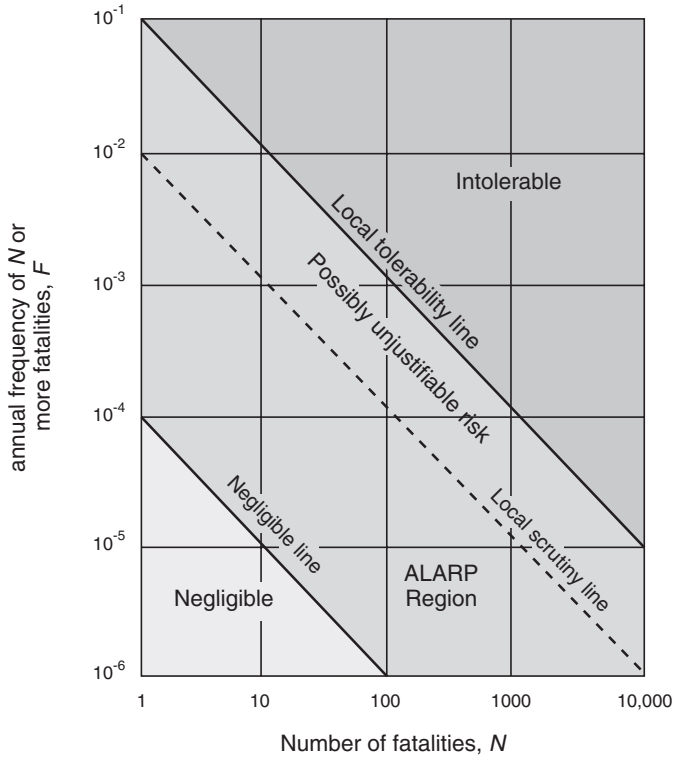


Figure 6.2: Societal risk tolerability. (After the UK Health and Safety Commission[7])

These risk limits were adopted without modification by the New Zealand Government's Special Committee on Nuclear Propulsion[8] to demonstrate its finding that the visits of nuclear-powered vessels to ports in New Zealand would be safe. The concept of upper and lower bands of tolerability, with a broad region where risks are treated to be as low as practical, has been adopted by the Environmental Risk Management Authority[9] as guidelines for assessing risks posed by hazardous substances and new organisms. The Authority, however, has not put quantitative values on these risk limits at the time of writing.

Case Study 6.1 describes another way of setting an acceptable risk boundary in terms of the extent of accident and its impact on people.

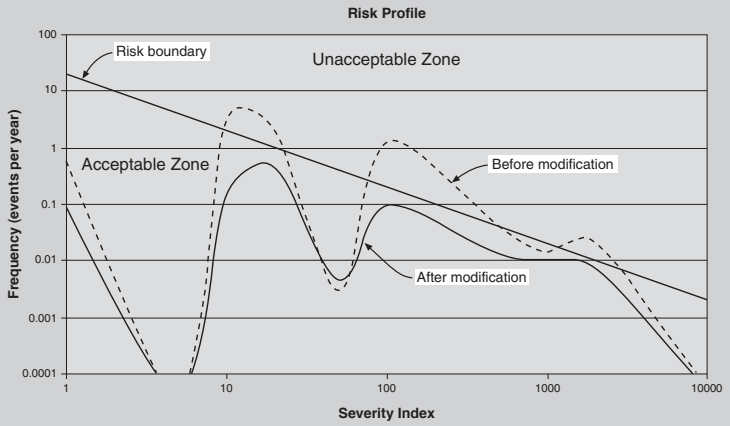
Case Study 6.1 Environmental Risk Assessment of a Proposed Wastewater Treatment Plant
(Bermingham, 1999, *pers. comm.*; courtesy, Watercare Services Ltd)

Watercare Services Ltd, Auckland, wished to quantify the risks associated with the operation of the proposed plant at Mangere. In addition, some basis for developing Emergency Response Procedures was required.

Owing to the wide range of ways that the environment can be affected, a "bottom up" event-tree approach was taken, combined with an environmental consequence model, to evaluate possible incidents.

The waste treatment plant process was first split into discrete stages that represented the major process steps and plant services. A standard list of hazards was developed and applied to each stage. Wherever applicable, the consequence of each hazard, and the expected frequency of occurrence was considered and the resulting faults noted. The effect of mitigation and contingencies was factored in and the estimated environmental effects listed.

The effect on the environment was measured in terms of public perception and simplified by describing effects in terms of discrete measures of duration of effect and the extent (area/number of people affected). Each step in consequence was assigned a Severity Index. A proposed Resource Consent limit, expressed as a percentage time that limits could be exceeded, allowed an acceptable risk boundary to be set.



Outputs of the study were:

- Identification and ranking of the fault sequences that represented highest risk.
- Mean Time between Failure (MTBF) criteria for critical process elements.
- Graphical representation of the plant's risk profile
- Identification of unacceptable risks in terms of the incident type.

The information derived from the study was available to the process designers thus enabling the design to be refined to the point were environmental risks could be reduced to an acceptable level by the most efficient means.

Society's aversion to multiple-fatality accidents has sometimes been translated into formal criteria such as those adopted by the Danish and Dutch authorities (Stallen et al.[10]). In the Netherlands, for example, it is proposed that the societal risk shall be less than the limit given by

$$f \leq \frac{C}{N^2}$$

where f is the accident frequency, N is the number killed in a given accident and C is a coefficient which represents society's accident tolerance. The Dutch have chosen 0.001 for the value of the coefficient, whereas a taskforce of Danish engineers have recommended a value of 0.01 in respect to the siting of chemical plants (Taylor et al.[11]). Pikaar and Seaman[12] report that a number of major European chemical companies now apply societal risk criteria in the internal self-regulation of their activities.

As in the United Kingdom, risk-tolerance limits have been proposed in the Netherlands for town-planning purposes in the neighbourhood of the transport routes for hazardous materials (Stallen et al.[10]). However, an attempt to formulate a similar limit in connection with the development of a fifth runway for the country's major international airport failed because of differences in the nature of the hazards and the areas of exposure between airports and fixed process installations.

The Anglo-Dutch risk-assessment developments have been applied in other countries, usually on an ad-hoc basis; but in New South Wales, the Department of Environment and Planning has adopted criteria specifying a variety of maximum allowable risk levels not to be exceeded for individual risk from a limit of 10^{-6} per year in residential areas and a limit five times higher in industrial zones[13]. Similar attempts to set risk guidelines for the siting of LPG facilities did not gain acceptance in New Zealand.

For geotechnical hazards, Fell and Hartford[14] provide suggested tolerable fa-

tality-risk criteria for the individual risk from landslips involving engineered slopes. These values, set out in Table 6.1, appear to have been based on other criteria for existing, new and upgraded dams (ANCOLD 1997). The situation for natural slopes is less clear. Fell and Hartford[14] speculate that the general public will tolerate much higher individual risks from unmodified slopes and suggest a criterion of order 10^{-3}. While the public may be more tolerant of failures on unmodified land, such failures are less likely to have human impact in many cases. If valuable, non-human resources (such as infrastructure) are mainly at risk, then a much higher probability would seem to be more appropriate, or a cost-based criterion chosen.

Table 6.1: Criteria for tolerable individual fatality risk from landsliding (after Fell and Hartford[14])

Situation	Tolerable risk for loss of life
Existing slopes	10^{-4} for person most at risk 10^{-6} average of persons at risk
New slopes	10^{-5} for person most at risk 10^{-6} average of persons at risk

Farmer's risk profiles are given in terms of risk of death. There are reasons for choosing fatality criteria. Data on fatalities are recorded by law, but information on levels of injury is more difficult to interpret even when available. However, in any given occupation, there is generally a correlation between lost-time and injury accidents and those which result in death. The triangle of accidents, Figure 5.5, illustrates this principle. Measures to reduce the incidence of fatal accidents will also reduce the likelihood of accidents of lesser gravity being witnessed.

There is clearly a limit to the extent of reliability, even with best engineering practice, and also the degree of confidence in estimates put on that reliability. Bowen[15] quotes a limiting figure of 1 event in 100 000 years is the failure probability to which plants can be engineered on the basis of experience in the nuclear power industry. Lees[16], in commenting on this figure, notes that a distinction should be made between an estimate of 10^{-5} per year, as a single figure, and one that has been made as a compound of two separate events, with risks of 10^{-2} and 10^{-3} per year respectively, for which a greater certainty may be put on the values. The point is acknowledged, but often a very small engineering probability is a compound of many more likely (and thus more certain) events.

Even more uncertain is the reliability that can be put on health risks obtained by extrapolating data from relatively high exposure levels to animal species or from the interpretation of accidental exposures. Unless there is a sound physi-

ological model of harm, or reliable epidemiological data, the method of extrapolation and the prudent safety factors to be embedded are essentially matters of professional judgement. As noted in Chapter 4, the extrapolation of bioassay data for ingestion of trichloroethylene in drinking water becomes very uncertain at low concentration levels[17]. For example, the range of estimated lifetime risks extends over four orders of magnitude at a concentration of 0.1 μg per litre. Nevertheless, even when the uncertainty is so high, as in this case, a risk-management decision based on data is likely to be sounder than one that has no physical basis whatsoever.

Risk Maps

Whenever a hazard potential is far-reaching, liable to affect many people, and the hazardous items are sufficiently separated that their individual contributions can be distinguished, the individual risks can be conveniently illustrated by superimposing contours of these risks (normally as annual probable fatalities) on a map of the area of concern. This is known as a *risk map*. An example for offsite risks is given in Figure 6.3, but risk maps may be used to pinpoint onsite hazardous zones[18].

A risk map only shows individual risk profiles. The whole picture of societal risk depends upon the population distribution as well. An individual fatal risk

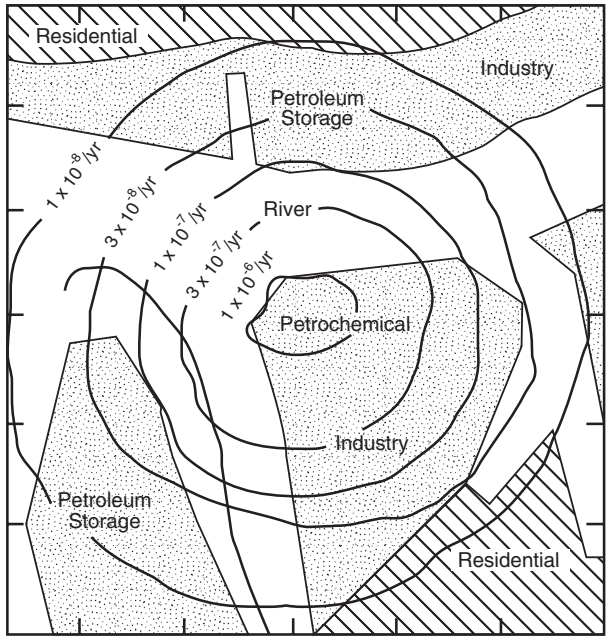


Figure 6.3: An example of an individual-risk contour plot or risk map (after Slater et al.[19])

of 2 x 10^{-6} (2 in a million) per year in a single detached house may be considered to be less serious than one of 0.5 x 10^{-6} (1 in 500 000) per year in a high-rise block of flats. Risk maps are thus used in conjunction with population distributions to represent risks to communities.

European planning authorities, notably in the Netherlands, have found risk maps to be a useful tool to assess the hazard potential of major industrial activity in densely populated areas, sometimes embarrassingly so. Gardenier (1998, *priv. comm.*) tells the story of one Dutch mayor who was proudly opening a new urban subdivision at the same time his officials were declaring that the land in question was in a zone above the limiting tolerable value for individual risk!

A risk map was first used in New Zealand by the Netherlands Safety Organisation, TNO, to show the risks associated with running an LPG pipeline through New Plymouth[20]. The surrounding area was divided into blocks of 100m size, and the effects of each unwanted event, such as a pipe rupture, were evaluated at every 100m along the length of the proposed pipeline. The societal risk was determined by assigning to each square a population on the basis that it was uniformly distributed throughout the residential area. The use of risk maps was found to be helpful by Stewart[21] in her comparison of natural and industrial hazards faced by a hypothetical New Zealand small town, but the risks from natural hazards were found to far outweigh those of industrial origin. Less detailed are generalised maps depicting natural hazard zones, such as those presented by the Christchurch Engineering Lifelines Group[22] in their study of the vulnerability of lifelines to natural hazards in the Christchurch metropolitan area. The zonal boundaries were drawn from geological information derived largely from numerous borelog tests.

Fatality Criteria

As noted earlier, fatality criteria have been frequently used as basis for comparing risks of various kinds. The *fatal accident rate* (FAR) is defined as the number of deaths per 10 million exposed hours, which is roughly equivalent to a workforce of 1000 being exposed over the whole of their working lives. Despite qualms about the equivalence of various kinds of risks[23], the use of fatal accident rates enables various risks to be compared on an equal contact-time basis. Such comparisons have proved to be useful means of eliminating the more risky activities and improving safety in the process industries overseas as well as in New Zealand.

The following Case Study 6.2 given by Kletz[24] illustrates the technique of using FAR values to assess safety levels.

Some FAR values for compensated accidents at work in New Zealand in 1981 are shown in Table 6.2. Although the data are fairly old, the relative ranking is

Case Study 6.2 Safety of Hydrocarbon-Storage Tanks

Maintenance records for 100 fixed-roof tanks for the storage of volatile hydrocarbons had shown that a total of 20 explosions or fires had taken place over a 20-year period. Four of these accidents had occurred when a worker was on a roof. The frequency of either fire or explosion per tank is thus given by 20 events / [1000 tanks x 20 years] = 0.001 yr^{-1}. The average aggregated contact hours between each incident is the ratio of the working hours per year to the number of incidents per year multiplied by the fractional exposure time (0.01). This gives a value of 2000 / [0.001 x 0.01] = 2 x 10^8 hours for this averaged period. Since the unit value of FAR corresponds to a contact time of 10^8 hours, the FAR value is 1/2. This is small compared with the mean value for the industrial hazards in the chemical industries, and might be regarded as indicating a tolerable risk. However, the presence of a worker on the roof may lead to a greater chance of an outbreak of fire or explosion due to that worker's activities there. The conditional probability for a fatality given an accident is 4/20 = 0.2, whereas the conditional probability for a worker to be on the roof is only 0.01. Clearly, the presence of a worker on the roof had increased the chance of an accident twentyfold (0.2/0.01), and the risk now appears unacceptable. On the basis of this calculation, the tanks were fitted with nitrogen blanketing to reduce the hazard.

still likely to hold. These data may be compared with others for non-occupational activities listed in Table 6.3.

The notable thing about these data is that many everyday activities appear to be riskier than some occupations that are considered be quite hazardous (such as high-rise construction) when activities are compared on a equal contact-time basis. One explanation may be that most of us only undertake our riskier ventures in bursts of activity. This point is illustrated by a speculative example of a person's possible weekly spread of activities (Table 6.4). The risks associated with everyday activities are "shared" so that the relative risk for each is about the same. This principle of risk aversion can be used in regard to occupational hazards, in which working practices are regulated so that high-risk activities are moderated by the minimisation of contact time in the hazard zone.

Table 6.2: Compensated fatal accidents at work in New Zealand in 1981 (after Keey[25]). A FAR index of 1 corresponds to 1 death in 10^8 (100 million) hours exposure

Occupation	FAR index	Occupation	FAR index
Consumer and tourist services	3.4	Construction	8.2
Finance, banking and insurance	3.5	Transport, storage and communication	13.9
Manufacturing	3.8	Agriculture, forestry and fishing	16.4
Community and social services	4.5	Mining and quarrying	23.1

Table 6.3: FAR index for non-occupational activities (adapted from Kletz[24] and Smith[26])

Activity	FAR index
Staying at home (8h/day)	3
Travelling by bus	4
Travelling by train	5
Travelling by motor-car	50-60
Riding a pedal bike	100
Travelling by air	100-250
Riding a motor bike	500-1000
Canoeing	1000
Swimming	1300
Mountaineering (rock-climbing)	4000

Table 6.4 : Risks of everyday living, a speculative example

Activity/Exposure	FAR	Contact hours per week	Weighted FAR
Sleeping	0	56	0
Activities at home	3	63	1.1
Activities at work	7	40	1.8
Driving	60	5	1.8
Recreation	50	4	1.2
Total			5.9

It follows that there is a danger in comparing averaged work-related risks with those of recreational activities which are enjoyed only for brief periods for the element of danger that are associated therewith. Averaged data can obscure the hazards of particular jobs, as such data mask the hazards of the things we do after work. Nevertheless, industrial health risks of certain trades can be high. Carson and Mumford[27] report FAR rates varying from 3 for cancer of the scrotum for turners with cutting oils, 35 for nasal cancer for wood machinists, and 325 for cancer of the bladder with rubber-mill workers. About 8% of all cancers reported in 1980 in the United Kingdom were attributed to exposures at work.

Injury Criteria

While the use of fatal-risk criteria seems straightforward and relatively easy to compare with other hazards in life, there are still a number of problems in to-

tally relying on these criteria alone. The United Kingdom's Health and Safety Executive[7] notes that:

- Society is concerned about risks of serious injury or other damage as well as death;
- There are technical difficulties in calculating the risks of death from a hazard to which individual members of a population may have widely different vulnerabilities;

and one might add:

- In New Zealand, the number of fatal accidents attributed to engineering failures are rare, and work-related deaths are less common than traffic accidents (by an order of magnitude).

The Health and Safety Executive[7] suggests that an injury criterion might be based on the concept of an excessive dose, which might be a "dose" of excess heat from a fire, an overpressure from an explosion or exposure to a toxic material, giving all of the following effects:

- severe distress to everyone;
- a substantial fraction requiring medical attention;
- some people being seriously injured, requiring prolonged treatment;
- any highly susceptible people being killed.

Keey[28] also adds serious disruption to lifestyle, including an evacuation lasting for more than 1 hour. With this approach, a quoted risk level (such as 1 in a million per year) would represent the likelihood of receiving a "dose" from a one of a wide range of possible events. Some events may give doses within a risk target, while others may yield a worse dose. In analysing these risks, assumptions have to made regarding typical occupancy of areas under threat. Individual and societal risks differ whenever buildings are used continually by the same people (as in workplaces) rather than intermittently (by shoppers in supermarkets, for example).

A figure of 1 in a million per year was proposed as the lower bound of tolerability in relation to the risk of receiving a dangerous dose or worse for a typical pattern of user behaviour in a proposed development. (The Health and Safety Commission[7] added that this bound corresponds to a risk of about one-third in a million per year death, estimated on the basis of the risk of getting a somewhat higher dose which would result in the death of one-half of the exposed population). For developments where there would be clearly a large proportion of highly susceptible people, such as rest-homes for the elderly, a lower bound of one-third of a million per year was suggested as the tolerable limit for getting

a dangerous dose.

Injury accidents are reported as the number per 100 000 exposed hours, corresponding roughly to a single working lifetime, or as an annual rate per 1000 persons, as listed in Table 6.5. The number of injury accidents of varying severity seen for every fatal accident ranges approximately between 50 and 1000, depending upon the nature of the hazardous activity or situation.

Table 6.5: Compensated accidents at work in New Zealand in 1981 (Keey[25])

Occupation	Rate per thousand		Injury/fatal accident ratio
	Fatal	Non-fatal	
Agriculture, forestry, fishing	0.304	25.7	84.5
Mining & quarrying	0.430	85.3	198
Manufacturing	0.071	59.9	844
Utilities	0	51.2	-
Construction	0.152	39.8	262
Transport, storage, communication	0.260	40.7	157

Organisational Factors

Deficiencies in management can lead to degradation of safety levels though poor management policies and deficient feed-back of information about working conditions, as shown in Figure 6.4. This failure may be due to inadequate auditing or reporting of accidents, but could also derive from the absence of local checks and strategic controls.

There have been attempts, therefore, to account for management-related parameters in quantitative risk assessments. For example, Bennet[30] suggests the use of a management factor as a multiplier to calculated hazard indices to take account of four elements in a safety-management system which influence a worker's ability to do a job: the training procedures, the standard of equipment and instrument maintenance, the standard of control-system hardware and the quality of safety management. These elements are then graded against verbal descriptors ranging from 0 for "poor" to 1 for "excellent". The management factor *MF* is then given by

$$MF = \frac{1}{\sum_{j=1}^{m} w_j R_j}$$

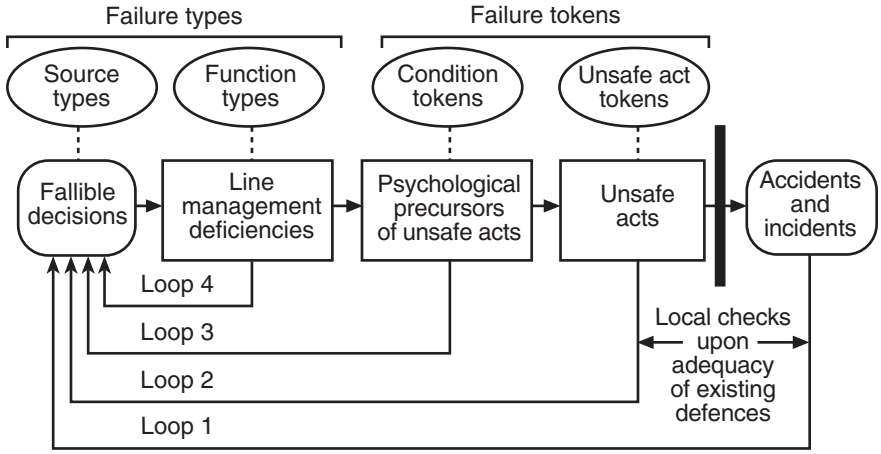


Figure 6.4: Influence of organisational factors in the degradation of engineering safety (after Tuli and Aplostolkalis[29])

where w_j is a weighting and R_j is the rating of the j^{th} management element. Bennet suggests a uniform value of 0.5 for the weighting factor, so that an "average" management factor based on an "average" rating of 0.5 yields a unit value for *MF*. "Fair" ratings result in a value of 2.5 for *MF*, which is consistent with Kletz's observation[31] that a management factor range of at least 3 is needed to account for normal differences in management skill. A more elaborate scheme has been proposed by Keey[25] based on a ten-point evaluation with differences in weightings.

The concept of a management factor is embedded in the evaluation of the instantaneous annual fractional loss developed by the Insurance Technical Bureau noted in Chapter 5. However, while insurance companies may be able to devise a scale based upon the loss history of their clients, it is generally more difficult to estimate numerical values of an adjustment factor on published failure and accident data which presumably correspond to some average standard of management. Further, Tweeddale[32] argues that it is unsound to multiply generic failure rates by some overall management factor. The cause of any failure or accident is due to particular circumstances, usually involving abnormalities and lack of mitigation. Although Tweeddale tentatively suggests the hardware and human failures might be separately estimated, with different management factors for each kind of failure, he concludes that failures due to human causes are so indeterminate that the risk assessment becomes essentially unquantifiable in this way. He recommends that the integrity of a quantitative risk analysis should be preserved, with the hardware-related failures estimated quantitatively and the rest of the risk assessment being treated qualitatively.

The problem cannot be so simply resolved, because recorded hardware-related failures contain other embedded factors. In a pioneering survey of process-plant maintenance records, students[33] from Loughborough University in the United Kingdom tried to determine basic failure rates for control and measurement instruments by estimating a so-called "*environment factor*", which varied from 1 in clean, well-managed conditions to 4 in the worst cases. Rarely have subsequent workers attempted to copy this approach, and the published data represent some kind of average of past practice.

Risk-evaluation Case Studies

The following case studies illustrate examples of risk evaluation of varying complexity.

Case Study 6.3(a) Liquefied Petroleum Gas Storage and Distribution Facilities

Vocal concern about the possible widespread introduction of bulk liquefied petroleum gas (LPG) into New Zealand resulted in the proponent company, Liquigas Ltd, commissioning a series of site-specific reports for the proposed storage and distribution facilities from A D Little Inc. whose work was subject to an independent academic audit. Separately, the former Liquid Fuels Trust Board[20] commissioned its own report from the Industrial Safety Department of the Netherlands Organisation for Applied Scientific Research, TNO. This study, besides assessing the risks and town-planning implications of LPG use, also reviewed the safety record in countries with long-standing experience with the fuel. The work relied heavily on a much larger risk assessment undertaken for the Netherlands government to provide guidelines for planners and other officials in defining requirements for the siting, design and construction of LPG facilities. It was a major study, costing some NZ$2.5 million, and described in a 27-volume, 4000-page report.

This detailed risk analysis enabled the safety aspects of various alternative systems to be considered such as:

- the comparison of above-ground storage with mounded or underground storage;
- the comparison of alternative transport options, such as the use of pipelines or movement by coastal tanker;
- the comparison of alternative road-transport routes, such as a shorter route though a shopping area with a longer route through a more residential area.

These comparisons led to the choice on safety grounds for mounded tanks at storage depots rather than above-ground cylindrical or spherical vessels.

The various risk analyses differed in their numerical estimates of the impact of rare, far-reaching effects, due to possible differences in the embedded pessimism in the effects models chosen, but all agreed that major incidents were most unlikely given the design criteria to be adopted and the assumption of high standards for maintenance of the proposed system. Inevitably with such large studies, critics were able to point to some inconsistencies, and one assiduous witness at the hearing for the proposed developments in Christchurch pointed to an order of magnitude error in the calculations for the

safety of the tankship when berthing in Lyttelton harbour. In the end, the multiple safeguards illustrated in the various fault trees were more persuasive of safety than the numerical estimates of top-event frequencies.

Case Study 6.3(b) Petroleum Transportation Hazards in the Wellington Region (Brabhaharan, P and Gnana Bharathy, Opus International Consultants, 2000, *pers. comm.; courtesy, Wellington Regional Council*)

The aim of this study was to determine the nature and spatial distribution of risks associated with the transportation of petroleum products in the Wellington Region, by sea, road, rail and pipelines. The adequacy of existing controls and response systems was to be considered, to assist in planning for risk mitigation and emergency management.

Simplified event trees were used to combine the probabilities of related contributory events, with traffic analyses to determine accident potential. The spatial distribution of risk was assessed using a Geographical Information System (GIS) for combining the hazards with the consequences, and for presenting the risks.

This risk study enabled an objective assessment of the risks to the community and the natural environment from petroleum transportation, and presentation of the risks spatially using a GIS. This will enable the use of these risk maps in planning for risk management, including mitigation at critical areas and emergency preparedness.

Case Study 6.3(c) Rosebank Industrial Area

In 1988, Auckland City Council commissioned an investigation into the levels of risk from industrial activity in the Rosebank Peninsula. The study was a response to a growing concern about the use of hazardous materials, particularly those close to residential developments and sensitive areas of the natural environment. The industrial area is confined into a narrow landmass which extends into the intertidal waters of the Waitemata Harbour and has limited access by road. Because of the large number of industries in the area, the scope of the study[34] was limited to ten representative installations, including chemical and paint manufacturing and warehousing, foundry, light engineering and metalworking plants.

Following a detailed site inspection, a list of potential incidents was drawn up and the possible severity and likelihood of each were estimated. The incidents were ranked and sorted according to type of impact, with judgemental scales of the effect on people, property and the environment. A fatality scale was used for the effect on people, with injuries and nuisance evaluated as fractional deaths. The effect on property was measured as the equivalent number of houses destroyed, while that on the environment in terms of the area affected and the persistence of the impact. While these scales were highly subjective, they enabled the various possible incidents to be ranked using the index:

risk index = (frequency) x (severity) x (chance of mitigation).

From this analysis, Wood and Tweeddale[34] concluded from the study that the hazards presented by the various industries were relatively small compared with industry worldwide. However, the likelihood of small-to-medium incidents, such as fires, was thought to be too high: some industries exhibited low safety standards and major deficiencies in safety management. The study illustrated the usefulness of what was essentially a scoping review in pinpointing those aspects which had the greatest need for improvement.

Case Study 6.3(d) Nuclear-powered Warship Visits

The New Zealand Government commissioned a special committee to report on the hazards should a nuclear-powered warship be present in one of the country's ports. The Special Committee[8] set out by considering the safety record of navies with nuclear-powered ships and comparing the safety standards of naval with land-based reactors. It consulted widely, and reported in considerable detail, including providing data on radionuclides in the environment and dose estimates from postulated accidents. It emphasised the importance of quality assurance for safety assessment, and was impressed by the safety-management regimes of both the British and United States navies. The Committee stated:

"When the likelihood of harm is so remote that it can occasion no rational apprehension, an activity may be regarded as safe."

In regard to a warship's presence in port, the Committee considered that the likelihood of harm was indeed extremely remote, and thus apprehension of harm was irrational. As Gardenier[35] in his review of the Report points out, the Committee did not explain at what level of risk apprehension becomes rational. He prefers the alternative statement:

"When the likelihood of harm is so remote that, **in the light of its potential magnitude**, it does occasion no apprehension, an activity may be regarded as safe".

This difference of opinion highlights the need to separate the expert assessment of hazards from a judgement on their tolerability by society.

Case Study 6.3(e) Tranz Rail Network Study

As noted in Case Study 2.4, Peet and Ryan[36] discuss the application of risk-assessment techniques to the operation of New Zealand's rail network. Their paper examines various methods used to evaluate the hazards of train collisions, such as those between trains, those involving road vehicles at level crossings, those with and obstruction such as slip or washout and a tipover at a tight curve. The past history of such incidents provided a benchmark for a risk matrix, with a five-point scale for frequency and severity. The matrix gave some indication of the relative significance of the risks, but was unable to provide any information on the influence of controls such as signalling systems on the levels of risk. To gain such information, fault and event-tree methods were invoked. Peet and Ryan[36] note that development for a particular failure by means of a fault tree, which incorporates human, technical and operational features, leads to a better understanding of the quality of the system under investigation.

Other aspects of the network's operations which were considered included the transport of hazardous goods and the safety in the single manning of trains. Hazardous transport was evaluated using six-point scales of frequency and severity to yield hazard scores ranging from 0 to 36 as a basis for ranking the risks. Train-driver safety was assessed through fault-tree methods and comparing the evaluated risks with other industrial occupations using FAR criteria. However, safety for the locomotive engineer when dismounting from the cab in an emergency was assessed by a joint union/company working party without doing a detailed analysis.

The company, Tranz Rail Ltd, has gained a number of lessons from a decade of formal risk assessment. Since the development of fault trees requires considerable thought and investigation to ensure all possible sources of risks are accounted for, the methodology forces a deeper understanding of the way accidents happen. Quantitative risk assess-

ments show the relative importance of various factors influencing the risk and their interaction, while sensitivity studies can be done on critical components to understand more clearly the range of likely outcomes. The available data, however, may not be in the right form or lack consistency. Additional techniques, such as sampling of records or Hazop-like consultation, may be needed for their verification.

Case Study 6.3(f) Domestic Heated Water Tanks

Not all fault-tree analyses need be as detailed or as extensive as those developed in the study of railway operations. (The study reported by Peet and Ryan[36] for train-driver risks involved 20 major trees and 200 inputs!) By contrast, only two fault trees with 15 inputs were needed by Powell[37] in her study of the explosion risks of domestic, heated water-storage tanks. The investigation for the Building Research Association was concerned with the need for additional safety by using a combined temperature and pressure-relief valve on low-pressure, valve-vented tanks rather than the current practice of relying on pressure relief alone. The analysis drew attention to two interesting points about the use of temperature/pressure relief valves: common-mode failures such as blocking and incorrect installation could decrease the effectiveness of the these valves; while the high-temperature setting of one tested valve might have allowed steam to be generated during periods of low-pressure weather without any relief action. There seemed to be little gain in safety by requiring a change to current practice.

References

1 Slovic, P, Fischoff, B and Lichtenstein, S (1981): "Perceived risk: psychological factors and social implications", *Proc. Roy. Soc. London, A 376, 17-34.*

2 Lee, T R (1981): "Perception of risk: the public's perception of risk and the question of irrationality", *Proc. Roy. Soc. London, A 376, 5-16*

3 Sabey, B E and Taylor, H (1980): "The known risks we run: the highway", in Schwing, R C and Albers, W A Jnr (eds), "*Societal Risk Assessment: How Safe is Safe Enough.*", 43-70, Plenum Press, New York London.

4 Farmer, F R (1981): "Quantification of physical and engineering risks", *Proc. Roy. Soc. London, A 376, 103-119.*

5 Rothchild, Lord (1978): "Risk", *The Listener, 100, 715.*

6 Provinciale Waterstaat Groningen (1979): "Pollution control and use of norms in Groningen" (Nota millieunormen provincie Groningen), PW Groningen.

7 Health and Safety Commission (1991). "*Major Hazard Aspects of the Transport of Dangerous Substances*", HMSO, London.

8 Special Committee on Nuclear Propulsion (1992): "*The Safety of Nuclear Powered Ships*", Dept of the Prime Minister and Cabinet, Wellington.

9 Environmental Risk Management Authority (1998): "*Methodology for the Consideration of Applications for Hazardous Substances and New Organisms under the HSNO Act 1996*", Final proposal Jan. 1998, ERMA New Zealand, Wellington.

10 Stallen, P J M, Geerts, R and Vrijling, H K (1996): "Three conceptions of quantified societal risk", *Risk Analysis, 16, 635-643*.

11 Taylor, J R, Kampmann, J, Kragh, E K, Becher, P and Petersen, K E (1989): "Quantitative and qualitative risk criteria for risk acceptance", *Rep. Miljøstrelsen, ITSA, Roskilde, DK*.

12 Pikaar, M J and Seaman, M A (1995): "A review of risk control", *Rep. SVS 27A*, VROM, Den Haag.

13 Gardenier, J (1992): "General concepts of risk", in Gardenier, J and Keey, R B (ed.) "*Risk Assessment of Natural and Industrial Hazards", pp* 11-32, CAE, Univ. Canterbury, Christchurch.

14 Fell and Hartford (1997). Reported in *BRANZ Study Report No 83*, 1999.

15 Bowen, J H (1976): "Individual risk vs public risk criteria", *Chem. Eng. Prog*. 72 (2), 63.

16 Lees, F P (1996): *"Loss Prevention in the Process Industries",* 2nd edn, Butterworth-Heinemann, London.

17 Cothern, C R , Coniglo, W A and Marcus, W L (1986): "Estimating risk to human health", *Environ. Sci. Technol., 20(2),* 111-116.

18 Sanders, K A (1992): *"Production and evaluation of safety assurance software for process industrial sites in New Zealand"*, ME thesis, Chem. and Proc. Eng., Univ. Canterbury Christchurch.

19 Slater, D H, Corran, E R, Pitblado, R M (1986): *"Major Industrial Hazards"*, Project Rep., Warren Centre, Univ. Sydney NSW.

20 Liquid Fuels Trust Board (1984): *"Risk Assessment of Future LPG Facilities in New Zealand"*, Rep. No. LF 5006, LFTB, Wellington.

21 Stewart, J C (1994): *"Risk assessment of natural and industrial hazards"*, BE Rep., Chem. and Proc. Eng., Univ. Canterbury, Christchurch.

22 Christchurch Engineering Lifelines Group (1997): *"Risks and Realities"*, CAE, Univ. Canterbury, Christchurch

23 Gough J D (1988): *"Risk and Uncertainty"*, Inform. paper, no. 10, Centre for Resource Management, Univ. Canterbury & Lincoln College.

24 Kletz, T A (1971): "Hazard analysis - A quantitative approach to safety", *IChemE Symp. Ser., No. 34, 75-81.*

25 Keey, R B (1987): "*Reliability in the Process Industries*", IPENZ, Wellington.

26 Smith, D J (1993): "*Reliability Maintainability and Risk*", 4th edn, Butterworth-Heinemann, Oxford.

27 Carson, P A and Mumford, C J (1986): *Loss Prevention Bull. No.067*, IChemE, Rugby.

28 Keey, R B (1991): "A rapid hazard-assessment method for smaller-scale industries", *Proc. Safety & Environ. Protection, 69(B2), 85-89.*

29 Tuli, R W and Apostolakis, G E (1996): "Incorporating organizational issues into root-cause analysis", *Proc. Safety & Environ. Protection, 74(B1), 3-16.*

30 Bennet, A J (1992): *"Rapid ranking of process hazards"*, unpublished, Chem. and Proc. Eng., Univ. Canterbury, Christchurch, reported by Sanders, K A (1992).

31 Kletz, T A (1985). "Estimating potential hazards", *Chem. Eng.*, 1 April, pp 48-68.

32 Tweeddale, H M (1992): "Balancing quantitative and non-quantitative risk assessment", *Process Safety and Environ. Protection, 70(B2), 70-74.*

33 Anyakora, S N, Engel, G F M and Lees F P (1971): "Some data on the reliability of instruments in the chemical plant environment", *Chem. Engr. No. 255, 396.*

34 Wood, S and Tweeddale, H M (1990): "Rosebank Peninsula risk assessment study - A review of safety and risks in an Auckland industrial area", *Proc. Annual Conf. IPENZ Auckland, II, 51-61*

35 Gardenier, J (1993): "*Report on nuclear powered ships. A credible proof of negligible risk*?", (unpublished), Wellington.

36 Peet, W and Ryan, R (1998): "Risk management in a network operation: understanding complex systems", in Elms D G (ed.) "Integrated *Risk Management*", CAE, Christchurch.

37 Powell, L (1995): "*Explosion risk analysis for valve-vented storage water heaters*", BE (Chem.& Proc.) Rep., Univ. Canterbury, Christchurch.

7 Risk Communication and Treatment

Risks cannot be treated properly unless they are communicated. Lord Cullen[1], after the public inquiry into the disaster that destroyed the oil platform, Piper Alpha, wrote:

> *"The top men in Occidental were not hard-nosed and uncaring people interested only in profit and unconcerned about safety. They said and believed all the right things, (but) they did not get involved in the precise actions required, see that they were carried out and monitor progress."*

Senior technical managers, who may not be qualified engineers, have a major influence on the management of engineering risk, and there is a professional responsibility on engineers to ensure that the levels of engineering risk associated with their work are fully communicated.

In the case of the *Challenger* disaster described in Case Study 2.2, senior management were not well enough informed to appreciate the significance of the concerns being expressed by the technicians and engineers. *Good communication demands a clear speaker and a willing listener*.

Another example of the harmful effect of poor internal communication was the loss of a North Sea ferry, when senior management ignored earlier and repeated representations about hazards. The background to this disaster is briefly described in Case Study 7.1. The need for safety awareness at senior levels is the concern of the IPENZ policy statement entitled *Risk and Prudence* on engineering governance that has been mentioned in Chapter 1 and reproduced in Appendix B.

Besides internal communication of risk, external communication is becoming crucial. Over recent years the public has become more aware of and concerned about technical hazards, and recent, well-publicised failures in New Zealand and Australia mentioned in the Preface have raised questions regarding the reliability of engineering systems. Part of this concern has arisen because of hardening public attitudes to safety and the protection of the environment with a mistrust of technical solutions. Engineers, in exercising their profession, now need to be fully aware of these issues.

The purpose of risk communication in any risk-management policy is to make sure that all stakeholders and parties involved understand the risks and associated benefits, the options for treating risk, and the requirements to implement them.

Effective risk communication is a multiple dialogue in the search for solutions.

Case Study 7.1 The Loss of the *Herald of Free Enterprise*

In June 1985, the master of one North Sea roll-on/roll-off vessel wrote to the directors of the ferry company, pointing out the absence of indicators to show the position of the doors on the car-deck. The deck was kept weather-tight by having both pairs of bow-doors and the single stern doors closed, the two sets of doors being closed manually from the car-deck. Small leaks, such as those from pipework and fire-fighting equipment, were removed by pumps. The master suggested that indicator lights should be fitted so that the positions of the car-doors could be confirmed on the bridge. The suggestion was rejected. In 1986, the master of a sister ship sent another request for door indicators, a request supported by the other master. The response from the directors remained negative. Prior to March 1987, the ferries sailed regularly with an excess load, with passenger numbers exceeding the licensed limit by several hundred people on many occasions during the summer. The ships' masters could only attempt to count passengers as they embarked or disembarked. The level of freight loading was also unknown to the ships' masters. This was a significant hazard because it affected the ship's trim and stability. Remote-reading draught gauges were not fitted, and it was alleged that draught measurements were falsified for the ship's log. When the issue of overloading was put to the directors, they did not respond.

On 6 March 1987, the *Herald of Free Enterprise* was loaded with 81 cars and 47 freight vehicles at Zeebrugge. The assistant bosun, who was responsible for closing the doors on the car-deck, had fallen asleep in his bunk after supervising maintenance operations. The ferry left the harbour with both the inner and outer bow-doors open. The bosun did not see it as his job to ensure that the doors were closed, even though he knew they were open. As the ship left the harbour under increasing speed, sea flowed into the car-deck and the pumps were quickly overwhelmed. The ship listed, the free movement of water causing it to capsize within four minutes, with the vessel coming to rest on her port side on a sandbank. While many persons were saved, 150 passengers and 38 crew died in the disaster.

Organisational Learning

Wells[2] notes that most organisations gather extensive amounts of information, much of it relating to safety. Such records include accident reports, data on lost-time injuries, comments on "near misses" and observations on dangerous procedures and practices. *This data collection should enable organisations to learn from the past to do better in the future*.

In a workplace, where permit-to-work systems are used for safety in maintenance, Iliffe et al.[3] recommend a computer-based system of issuing permits which could be linked to a database of incidents. Thus a user could be reminded of any special hazards associated with the equipment to be maintained, any earlier fault diagnosis (through a failure modes-and-effects analysis or other risk-identification tool), and have access to a parts inventory. The accident database might be structured within a *hierarchy of causes*, so that a person unfamiliar with a hazard can be prompted. For example, equipment cause might lead to identification of electrical equipment for which there has been cases of

short-circuiting or lack of earthing or overheating.

Investigation of major incidents, such as those described in Case Studies 2.2 and 7.1, reveal that *organisations sometimes have a culture of not wanting to know*. An organisation can respond to hazards by either denial or reform. An adequate and effective two-way channel of communication between all levels of management is essential to reduce the likelihood of significant risks being left untreated. Such communication can only work when *appropriately qualified persons with technical insight have positions at all levels in an organisation*, so that messages and information can be put into the correct context and appreciated. Violations of regulations should not be permitted or condoned, even if these rules are thought at the time to be impractical or burdensome in the pursuit of production and efficiency.

The Australian/New Zealand Standard AS/NZS 4360:1999 recommends that each stage of the risk-management process should be documented, including assumptions, methods, data sources and results. Such documentation demonstrates that the process has been properly conducted and provides a record to develop an organisation's database of knowledge that facilitates ongoing monitoring and review. It is a means whereby information can be shared and stored.

Communicating Risk

In reviewing conceptual approaches to risk communication, Pidgeon et al.[4] comment: *"At first sight, the task of communication might appear trivial given that most of us have little difficulty in conducting day-to-day interaction with colleagues, friends and associates"*. However, these observers note that risk communication involves talking with a number of audiences, who possibly hold diverse values within different frames of reference, and possibly have conflicting hidden agendas. Thus, at the outset, all groups and individuals who might be expected to be involved should be identified, and appropriate channels of communication arranged.

When a risk is established, the credibility of the chosen message-bearers is important, since all parties to the process bring their own biases. An apparent inventory loss of 170 kg of enriched uranium at a Scottish nuclear fuel-reprocessing plant appeared to have been dismissed by the management as an "accounting error", but this message was undoubtedly one factor in the decision announced by the United Kingdom's energy minister to close down the facility.

Pidgeon et al.[4] note that there are at least four overlapping conceptual approaches to risk communication:

- The top-down transmission of expert opinion to a non-expert audience;
- An interactive exchange of information and opinion among individuals,

groups or organisations;

- An exchange of information within a wider cultural or institutional context;
- A political process of empowering risk-bearing groups in society.

Whatever the view of risk communication, its effectiveness hinges on trust. *Trust is hard to gain, but easy to lose*. If the source of communication is not trusted, perhaps because the present evidence contradicts past messages, then it is unlikely that the new message will be trusted.

General criteria for good communication are set out in the Environmental Risk Management Handbook being prepared by an Australian / New Zealand Standards Committee, available in draft form in 1999. The objectives of good communication are: clarity, objectivity, timeliness and regularity. Although these objectives are sound in principle, they are difficult to achieve in practice.

Some of the basic rules of communication include:

- Write clearly and simply;
- Avoid hiding adverse information and be open;
- Take the initiative, especially when one has negative information;
- Avoid "killer words" such as *perfectly safe* and *risk-free* (which are never true) ;
- Quantify risk as far as possible;
- Acknowledge that there are no "dumb" questions;
- Be frank when dealing with the media;
- Be aware of factors that inspire trust;
- Put data in context and choose risk comparisons carefully;
- Remember that others will decide what is acceptable to them.

Particularly with major engineering projects, *it is easy to provide information overload in the attempt to be complete*. Normally, there are a limited number of matters of public concern. If these are seen to have been addressed appropriately, then the proponent organisation is more likely to be trusted that the whole project will be well-managed.

The legal obligation to consult with the public on engineering projects is discussed in Chapter 9.

Risk Treatment

Once any unacceptable risk associated with an engineering venture or process has been established with an adequate level of confidence, the various risk-treatment options should be identified and the appropriate strategy to bring the risk within target levels worked out. The Australian/New Zealand Risk Management Standard lists the treatment options as follows:

(a) *Avoid exposure to the hazard.* In manufacturing and processing activities, exposure to a hazard might be eliminated by introducing remote operation, or by replacing a dangerous facility with something that is more benign, or through using a less hazardous process involving less dangerous materials or operated under less arduous conditions. With existing facilities, such modifications can become expensive and deemed "uneconomic". Ultimately, poor technology is overtaken by something better. Costly retrofitting to meet safety standards can be avoided through adequate risk identification and consideration of alternatives at the start of an engineering project. It will always be cheaper to mitigate risks at an early stage of a project, and ideally at the conceptual stage.

(b) *Mitigate the impact.* The impact of a hazard may be mitigated by either reducing its likelihood (say, through the introduction of some control system to trip when a parameter reaches a critical value), or reducing its consequence should the hazard be realised by the installation of a protective shield. Any subsequent change to equipment or workplace practices must be scrutinised to check that the proposed change does not cause other risks by aborting or compromising the built-in safety features already installed.

(c) *Adapt to the hazard.* In dangerous work environments, such as high-rise construction, practices can be devised to reduce personal risk. In the case of handling dangerous materials, protective clothing can be worn and procedures changed to acknowledge the inherent dangers. Adaptation, in this sense, is a form of mitigation or minimisation of the hazard.

(d) *Duplicate resources.* Duplication of equipment enhances reliability by *introducing redundancy.* This is probably the commonest approach in many cases, and is a very effective option. The likelihood of experiencing the risk is thereby reduced, provided any standby or backup unit does not share a common element with the main unit.

(e) *Transfer the obligation.* Risk transfer is a contractual or financial instrument whereby responsibilities are transferred or an insurance policy is purchased, so that there is recompense in the event of an adverse effect. There is no change in the physical risk level, and normally this method of treating an engineering risk is used in conjunction with other measures to re-

duce the level itself. Risk transfer can ultimately be an expensive option if the transfer has been made to a wrong party or becomes burdensome.

(f) *Transform the risk*. This is another form of mitigation in which the risky process is transformed into one that poses less of a threat or may be more easily treated. Such procedures are sometimes adopted in treating environmental hazards generated by discharging waste streams containing contaminants: the hazardous material is captured in a form that can be more readily processed to less harmful products or recycled to the main process.

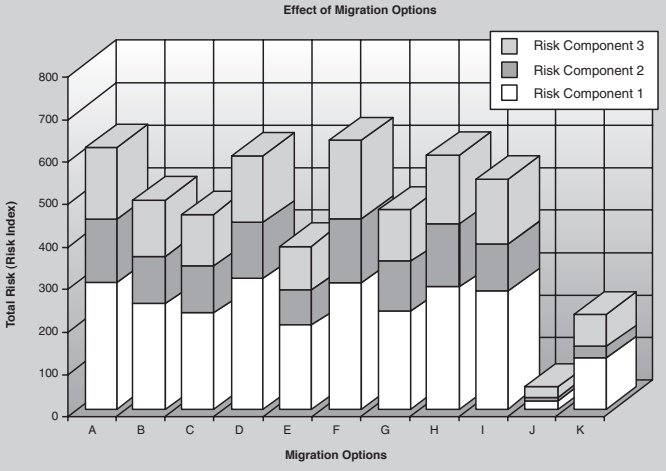
(g) *Retain the risk*. After risks have be reduced or transferred, there may be residual risks, which are retained by the organisation. Plans should be put in place to manage the consequence of the risk if they should occur, including a means of financing the risk. *Risks commonly are retained inadvertently or by default as a result of a failure to identify or treat them properly.*

Case Study 7.2 Risk Analysis of the Unintended Carriage of Dangerous Goods by Post (Bermingham, 1999, *pers. comm.*; courtesy, New Zealand Post Ltd)

The company was aware of the risks associated with the unintended carriage of dangerous goods by post. It needed to quantify the risk and to consider a range of possible risk mitigation options.

A model that simulated the factors that influenced the flow of mail was constructed. Limited quantitative data was compiled together with qualitative assessments of the effect of a range of mitigation options. This was applied to a systems model to compare the cost for implementation to the risk reduction achieved by each option.

The postal system was split into its essential parts following the flow of postal items and the sources of dangerous goods. A range practical mitigation options was identified following interviews with departmental managers. The experience of a range of employees was accessed through workshops to assess the probable effect of the mitigation options.



Mitigation costs were estimated separately. These data were combined with information on postal item flows to analyse the effect of the mitigation options.

The absolute numbers of dangerous good predicted by the study and the effectiveness of a number of the options were subsequently confirmed by trials and sampling of the mail flows.

Cost and mitigation information was plotted on a common grid to aid identification and implementation of the preferred options based upon the cost-effectiveness of risk reduction achieved.

The analysis demonstrated that the mitigation option chosen by some other postal services may not, despite the high associated cost, be achieving the intended reduction in risk exposure.

Risk Control

The Australian/New Zealand Risk Management Standard uses the term *risk control* to cover policies, procedures and physical changes that reduce the likelihood and consequences of risks. Risk control involves determining the relative benefit of new controls in the light of the effectiveness of existing controls.

In general, the alternative strategies for controlling risks would be evaluated in terms of their effectiveness in meeting safety targets, the costs to implement the various options and the impact of these control measures on stakeholders' objectives. The extent of this analysis will depend upon the magnitude of the hazard under review and the extent of its impact on the organisation or third parties. In some cases, the issue will be clear-cut, and the risk-control measures can be introduced as part of an engineer's normal responsibility in carrying out his or her work. *In other cases, a risk assessment may have far-reaching implications for an organisation*, and the various risk-treatment options would be documented and recommendations made for decision-making at a senior level.

Major risk-treatment plans would involve setting a timetable of implementation, the allocation of resources, detailing the staffing requirements and the development of a monitoring programme. Such monitoring would involve both periodic independent safety audits as well as reports of progress compared with budget and other project milestones.

As the Australian/New Zealand Risk Management Standard notes, it is unlikely that any one risk-treatment option will be a complete solution for a particular problem. Often an organisation will benefit substantially by adopting a combination of options, such as reducing the likelihood of risks, reducing their impact should they happen, and transferring them, retaining only the residual risks. An example of the latter is the effective use of contracts, with risk financing supported by a risk-reduction programme.

Project-Risk Treatment

Large engineering projects often involve financing transactions that involve a number of participants. Lenders rely for security principally on the assets of the project. As Gordon[5] points out, lenders are inherently concerned with the success of the project that they are financing and its ability to generate the planned revenue to repay its loan, they will seek to ensure that the project's financial risk to themselves is minimised and allocated, as far as possible, to other parties. The lenders will want assurances regarding the reliability of the engineering associated with the project, that the project will proceed smoothly to completion, on time and within cost, and the project will meet performance specifications.

The professional engineer (or engineering firm) may be expected to bear some risk in terms of liquidated damages and performance guarantees, which may be balanced by performance bonuses, giving the engineer (or firm) some incentive to bear the added risk. These risks, however, may in turn be spread to some extent to third parties, such as the suppliers or manufacturers of materials.

Risk Recovery

Risk treatment may be regarded as a preventative measure. It has the object of preventing a risk occurring, or reducing its likelihood of happening, or if it does, reducing its impact. On the other hand, risk recovery relates to the corrective measures that would be needed, should a risk eventuate, to bring the organisation's activity back to its former state. After a major event, the recovery would include reconstruction of damaged facilities and equipment and possible organisational changes. Risk recovery is carried out within a *predefined strategy* should the risk eventuate. By their nature, recovery strategies tend to be expensive, particularly when considerations of the potential loss of revenue are included. Moreover, reliance on risk recovery, rather than risk treatment, may involve questions of ethics.

Engineering Ethics and Professional Responsibility

The responsibilities of a professional engineer in regard to the treatment of risks is set out in the IPENZ Code of Ethics. He or she is expected to give priority to the safety and wellbeing of the community and have regard to this principle in assessing his or her duty to clients or colleagues. This ethic is not without its critics. While safety is an obligation placed on all engineers, not everyone agrees that it is foremost: at times, meeting a deadline or staying within budget may be given higher priority by some. *However, the Code of Ethics is clear about professional engineering responsibility to give priority to the wellbeing and safety of the community.*

Pinkus and her colleagues[6] note that *all engineering decisions involve trade-*

offs amongst performance, cost and schedules. Deciding what the nature of these trade-offs will be results from the tacit value judgments of the professional engineer. Because some degree of risk is inherent in all engineering work, an engineer is always striving to minimise that risk and maximise performance within the set schedule and permissible costs. Whenever a higher risk than that which is reasonably possible is accepted, defensible reasons are required to justify this action. *That is an ethical decision*. In this context, Pinkus et al[6] comment that NASA's decisions regarding how the space shuttle would be built, with cut-rate budgets, introduced pressures that led to an acceptance of a high-risk testing strategy into the programme. That strategy led to a degradation of reliability with a tragic and very costly outcome.

The acceptance of a high-risk factor may not of itself constitute a moral wrong. Two defensible reasons may be put forward for taking extra risks. First, those persons most immediately affected have been informed and have agreed to bear the risks. Secondly, the ultimate benefits of taking such risks are substantial and cannot be achieved in any other known way. The counter-arguments normally point out that those who would carry the risk are rarely those who would benefit.

Professional engineers are expected to be competent and responsible. A competent engineer is obliged, as far as it is reasonably possible, to be familiar with and understand the technology that is being used or is to be adopted. No one is expected to be omniscient in every aspect. The principle of individual competency extends to requiring persons to acknowledge areas where they are not competent or lack knowledge. However, it is reasonable to expect that large engineering organisations can have within their ranks, or can acquire, all needed competency. In this regard, the downsizing of in-house engineering expertise and added reliance on external consultants may cause some concern in maintaining levels of engineering competency within an organisation.

The responsibility of engineers extends to an obligation to voice their concern when an ethical dilemma has been identified. This may not be easy, particularly if voicing such concern can put an engineer at risk of losing his or her position, with major implications for the support of dependants.

References

1 Cullen, the Hon. Lord (1990): *"The Public Inquiry into the Piper Alpha Disaster"*, HMSO, London.

2 Wells, G (1997): "Major Hazards and their Management"*, IChemE,* Rugby, UK.

3 Iliffe, R E, Chung, P W H and Kletz, T A (1999): "More effective permit-to-work systems", *Proc. Safety & Environ. Protection, 77(B2), 69-73.*

4 Pidgeon, N, Hood, C, Jones, D, Turner, B and Gibson, R (1992): "Risk perception", in *"Risk: Analysis, Perception and Management", 89-134, Royal Society, London*

5 Gordon, C (1999): "Project finance can increase engineering risk", *NZ Eng 54(2),28-9.*

6 Pinkus, R L B, Shuman, L J, Humman, N P and Wolfe, H (1997): *"Engineering Ethics: Balancing Cost, Schedule and Risk"*, Cambridge UP, Cambridge.

8 Workplace Risk Management

Background

Over the centuries the workplace has been a dangerous place. The hazards at work have spawned many gruesome tales of enfeebled, maimed and killed workers. Occasionally there has been a happy ending, as in the tale told of a worker who, splashed with acid, jumped into the nearest emergency water-bath, which was solid with ice, it being mid-winter, skidded and broke his leg, but his fellow workers managed to wash him down before seeking medical help. Fortunately, he recovered from his serious burns and the broken leg, and afterwards married the attractive occupational heath nurse who had treated him!

Despite considerable improvements in occupational safety from the days of unfenced machinery and unventilated workrooms, there is continuing concern in New Zealand at the number of accidents in the workplace, particularly on construction sites. One response has been the industry-led initiative, *Worksafe*, to raise the awareness of hazards at work. There have also been calls for the Occupational Health and Safety Service of the Department of Labour to be more vigorous in prosecuting owner-occupiers in cases when accidents have revealed serious deficiencies in management and practice.

Examples of such deficiencies are revealed in three cases heard in early 1999 that are summarised in the Case Study 8.1.

Workplace health and safety is governed by the provisions of the Health and Safety in Employment Act 1992. At the time the bill was enacted, the total annual cost of occupational injuries, illness and disease was estimated at between $1 billion and $1.5 billion (OSH 1992). The Act places a duty of care on employers to ensure the safety and health of employees, and a responsibility was placed on employees to use safe working practices and ensure that their actions did not harm anyone else.

The method of managing workplace hazards associated with engineering activity is no different in principle from the generic process of risk management as set out in the Australian/New Zealand Risk Management Standard. This similarity is illustrated in Figure 8.1.

To assist in the development of an action plan in enhancing workplace safety, and meet the practical requirements in places of work, the Occupational Safety

Case Study 8.1 Three Examples of the Lack of Workplace Safety

- In the construction of a road viaduct, a worker was trying to disconnect a 400kg pump, which was suspended from a crane, when there was a failure of a link in the chain that was welded on to the top of its lifting point. The pump unit fell on to the worker, who received fatal injuries. The judge commented that the worker's employers should have spotted the visible flaws in the chain through their internal hazard-identification scheme, and the company was fined for not taking all practicable steps to ensure safety (The Christchurch *Press*, 31 March 1999).

- A worker was killed while undertaking maintenance in a steel-rolling mill. Access-gate switches, which would have turned off the machinery, had been replaced by warning signs and a register to be signed before working on the equipment. A company spokesman admitted that the arrangement was "an inexcusable failure of our safety practices" (*loc.cit.*), and the company was fined $35000, the highest penalty to that date for a single company under the Health and Safety in Employment Act 1992 (The Christchurch *Press*, 31 March 1999).

- A worker was operating a pelt-processing machine, when a pelt became stuck in it. To release the pelt, the worker removed the machine's protective guard. In the process, the worker slipped on a wet piece of plywood, accidentally depressing a foot-pedal which activated the machine, causing severe injuries to the worker's hand. The pedal had not been identified as a hazard by a consultant who had been commissioned to do an independent safety audit. The judge commented that such machines were "inherently dangerous" and, although the worker was partially to be at blame for the accident, the company ought to have taken steps to avoid it. On fining the company, the judge said that "he had to send a message to others in the industry that they must be proactive in avoiding accidents." (The Christchurch *Press*, 1 April 1999).

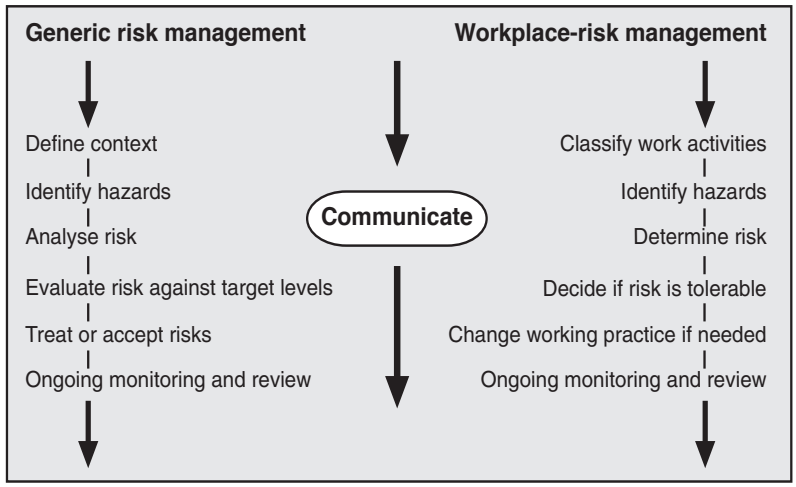


Figure 8.1: Chain of generic and workplace-risk management (after Bermingham 1999, pers. comm., with modification)

and Health Service has produced four booklets under the general heading of *Safety and Health is Good Business* 1992-4 as follows:

1. A Guide to the Health and Safety in Employment Act 1992;
2. How to Identify and Control Hazards;
3. A Guide to Managing Health and Safety;
4. Guidelines for the Provision of Facilities and General Safety in Commercial and Industrial Premises.

The *Guide to Managing Health and Safety* (3 above) emphasises the need for management to be committed to having an effective programme. Such commitment is reflected in the management's knowledge of the organisation's particular needs in safety and health, their conviction that high standards are attainable and the allocation of adequate resources to achieve those standards. This policy is enhanced by active employee involvement in the development of safe working conditions, since workers have both knowledge of the hazards at their place of work and are exposed to them daily.

Hazards that are assessed as "*significant*" present such a degree of risk that the Health and Safety in Employment Act requires a formal approach in dealing with them. A significant hazard is one that is an actual or potential source of harm:

1. That is serious (as defined in the first schedule of the Act), including permanent loss of bodily function, amputation, burns requiring referral to specialist medical services, loss of consciousness due to lack of oxygen, or accidents requiring a person to be hospitalised for more than 48 hours;
2. That increases with each exposure or with duration of the exposure to the hazards, such as noise-induced hearing loss;
3. That does not manifest itself or is not easily detected until a significant time after the exposure, such as asbestosis.

Methods of identifying, analysing and evaluating risks have been considered in greater detail in the earlier chapters of the book. The assessed likelihood and consequence of the identified hazards then leads to an action plan for treatment. In extreme cases, work should not be started or continued until the risk has been reduced. If that is impossible, the work has to be forbidden and abandoned. In less extreme cases, risk-reduction measures should be implemented within a set period of time. Whenever risks are considered tolerable, ongoing monitoring must be undertaken to ensure that safety standards and controls are maintained.

More recently, Standards New Zealand has issued an interim Standard (NZS 4801(Int):1999) to assist organisations in developing or adopting a management system for occupational health and safety (OSH). This provides a generic framework that can be easily integrated with other management systems as well as economic and other organisational goals.

Requirements for an OSH Management System

The fundamental requirement is that there should be an OSH policy authorised by the organisation's top management *that clearly states the overall objectives of the policy and a commitment to ongoing improvement of safety*. The interim Standard lists a number of features of such a policy. It shall:

1. Be appropriate to the nature and scale of the organisation's hazards;
2. Includes a commitment to continual improvement of the management system;
3. Includes a commitment to comply with relevant legislation and other requirements;
4. Be documented, implemented, maintained and communicated to all employees;
5. Be available to interested parties; and
6. Be reviewed periodically to ensure that it remains relevant.

A management plan for occupational health and safety defines those who are responsible for achieving the plan's objectives and targets and outlines the means by which these are to be achieved and the timeframe. All management personnel should be held responsible for occupational health and safety within the work areas under their control. The organisation, in consultation with the employees, should identify any training needs in regard to workplace safety and ways of performing work activities competently. Documents and data required should be readily located and updated, with obsolete documents removed or archived (with identification), as appropriate.

The implementation path involves commitment, planning and action, as set out in Figure 8.2.

The OSH method for workplace-risk assessment is a stepwise process:

1. The selection of the areas, tasks and processes associated with the places of work, and identifying hazards associated therewith (as outlined in Chapter 4);

2. Determining whether any injury, illness or damage could result from each identified hazard; and
3. Determine a potential severity and frequency rating;
4. Compile a risk-rating number (as explained below);

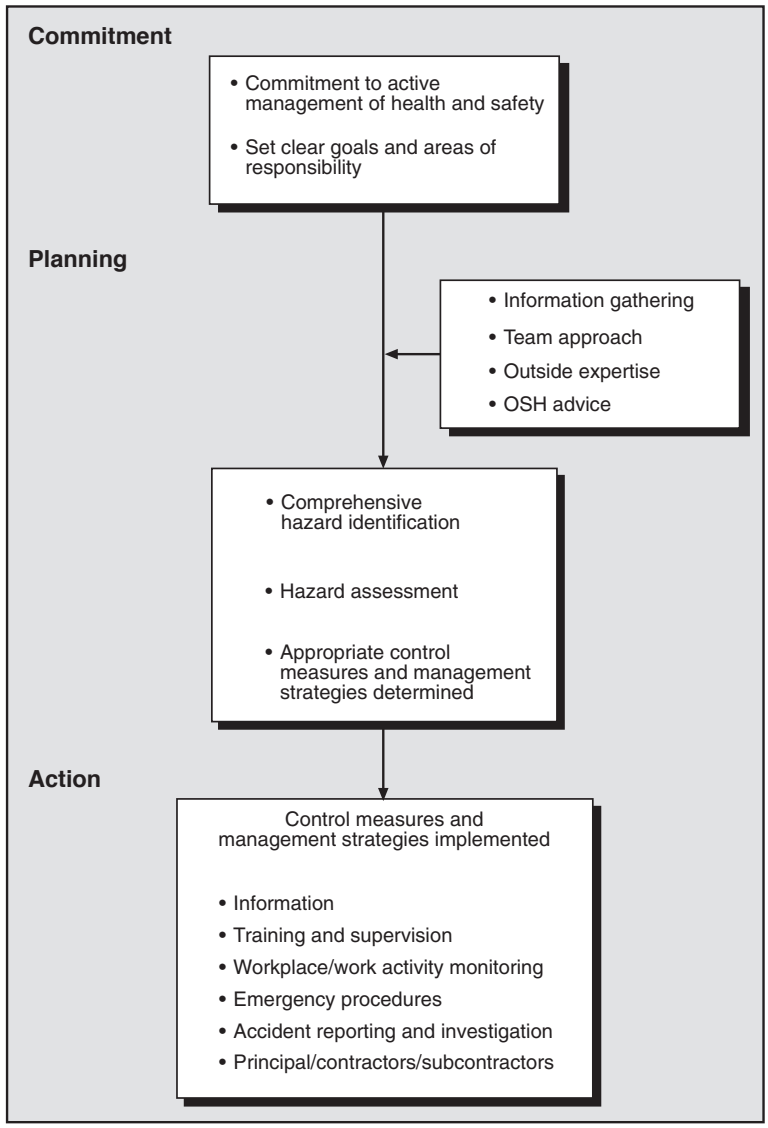


Figure 8.2: Implementation path for managing health and safety in the workplace (adapted from "A Guide to Managing Health and Safety", OSH, Wellington, 1993)

5. From the list of identified hazards and the risk-rating matrix separate the significant hazards from the others.

The risk-rating matrix is developed in a manner analogous to Gillett's scheme (Tables 5.1 and 5.2). The frequency is rated on a five-point scale:

1 Remotely possible.

2 Known to have happened in the past.

3 Strong likelihood of happening.

4 Happened previously within the organisation.

5 Happens frequently.

A four-point scale is used to rate the potential severity:

1 Negligible injuries or illness would occur.

2 Minor injuries or illness might occur.

3 Major injuries or illness would follow, including possible long-term disabling effects.

4 A fatality was likely.

These scores are then multiplied to get a risk rating on a scale from 1 to 20. This scale is not linear, but serves to rank hazards. The rating matrix is illustrated in Table 8.1.

Table 8.1: A risk-ranking matrix (OSH 1992)

Probable frequency	Estimated severity			
	4	3	2	1
5	20	15	10	5
4	16	12	8	4
3	12	9	6	3
2	10	6	4	2
1	4	3	2	1

This table should be interpreted with some caution, as it implies that a remotely possible hazard that might cause a death is to be viewed as being as serious as one of the lowest severity that has caused injury in the organisation at some

time in the past (since both have a risk index of 4). However, the risk scores provide some kind of rational basis to allocate resources in risk reduction by indicating those hazards that are of greatest concern. *Alternative matrices, such as those given in Tables 5.1 and 5.2, can be adapted to rate workplace risks, and may be more useful than the values given in Table 8.1.*

Based on the established level of risk, priorities for control are set, and the control mechanisms implemented, in a preferred hierarchy based on "reasonable practicality". Elimination is the first control method to be considered, followed by isolation and minimising the effects of the identified hazard. The use of guards to fence machinery has been the traditional method of isolating mechanical hazards at places of work. Chemical hazards can often be eliminated by using materials with more benign properties. If elimination is not possible, the risk should be reduced, such as the use of an electrical appliance of lower voltage or isolating or enclosing a hazardous appliance.

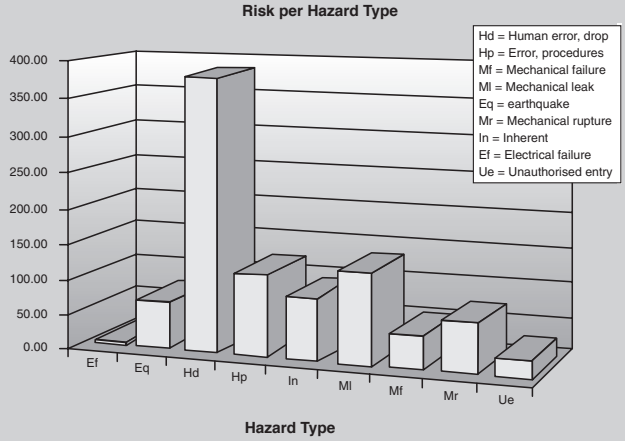
Case Study 8.2 Health and Safety Analysis for a Manufacturer
(Bermingham, 1999, *pers. comm.*)

A pharmaceutical manufacturer had been contracted to produce a new and highly toxic drug for an important international customer.

Due to the potential for harm to employees, the manufacturer had set up a safety committee and carried out a hazard identification study. A quantitative analysis was deemed necessary to allow a fuller understanding and assessment of the identified risks.

The safety concern was compounded by the uncertainties surrounding the health effects of the product to both normal and sensitised persons, as well as the complexity of the advanced process. It was considered that a quantitative study would allow both a better understanding of the true level of risk as well as a more structured identification of the appropriate mitigation options and their effectiveness.

The quantitative approach allowed the process's risk profile to be quantified and viewed in graphical form. The sources of risk were also displayed to focus further mitigation



efforts and ensure underlying trends were understood (shown above). In addition, the risk per employee was also derived and shown in graphical form to ensure that risks were spread and that no individual was exposed to an unacceptable level of risk.

Significant and highly cost effective reductions in risk were achieved as a result of the use of this quantitative technique.

Overall, a blend of technical and procedural controls is usually necessary. A decision tree for the control of hazards is illustrated in Figure 8.3. The control processes that are finally adopted are monitored by a documented evaluation of their effectiveness, and modified as necessary in the light of experience.

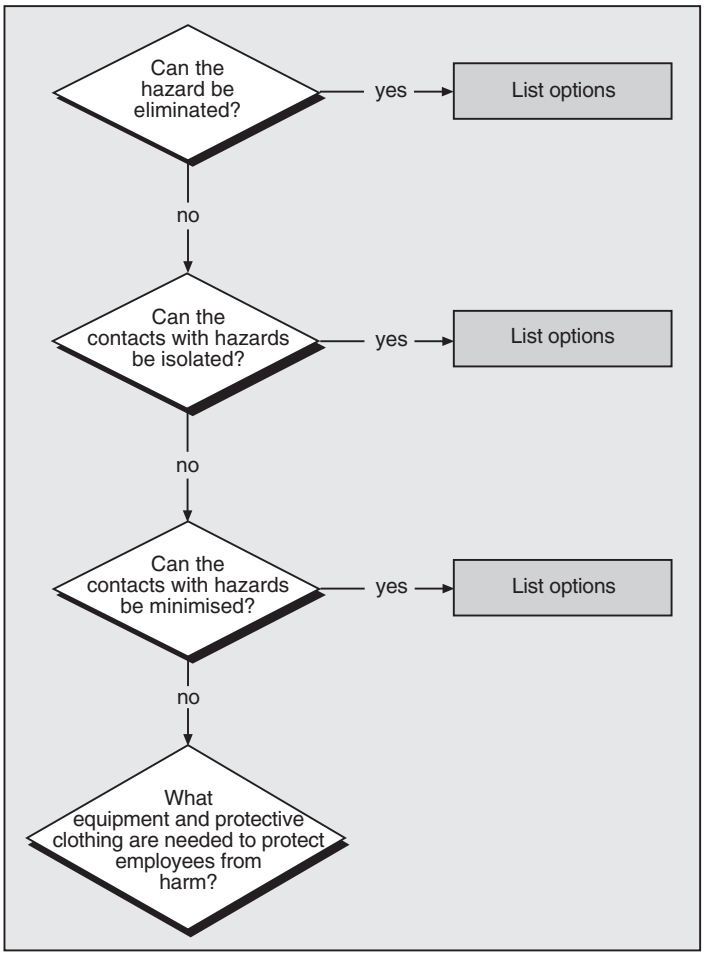


Figure 8.3: A hazard-control decision tree. (After Bermingham 1999, pers. comm.)

Reducing Unsafe Acts

A large number of accidents in the workplace stem from unsafe behaviour rather than breakdowns of plant and machinery. The accident triangle, as noted in Figure 5.5, has at its lowest level the presence of unsafe conditions and practices. If such unsafe behaviour can be reduced, the accident rate will fall also. This is shown diagrammatically in Figure 8.4.

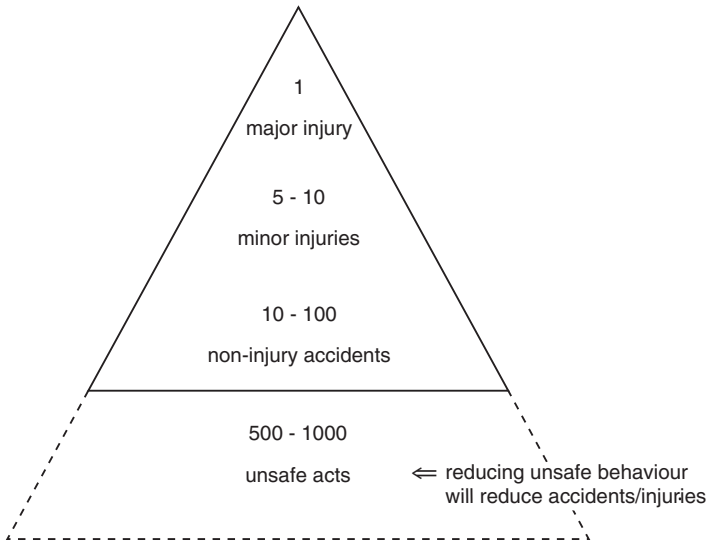


Figure 8.4: Accident/unsafe behaviour triangle

Three industrial psychologists[1] report that an analysis of earlier accidents in one company led to a clearly-defined list describing both safe and unsafe behaviour and, wherever possible, the outcome of the particular behaviour witnessed. Baseline examples of safe behaviour were observed and documented. These examples were then used in thirty-minute training sessions, when employees were shown slides demonstrating both the best and worst behaviour in various situations. The employees agreed to strive toward a goal of meeting baseline-safe behaviour for 90% of the time. Over succeeding weeks, behavioural safety improved and, over the first year of implementation of the policy, the injury rate dropped fivefold.

There is perhaps a natural desire to punish bad behaviour, perhaps as an example to others to do better. However, longer-lasting improvements are more likely to derive from safety self-awareness and the management's active promotion of a safety culture within an organisation.

Emergency Plans

When an organisation is confronted by an emergency, it is too late to then decide who needs to do what, the assistance that is available, and the response desirable. *Emergency plans must be developed beforehand*. They are, in fact, required under Section 6 of the Act, while Section 14 requires employees to be involved in their development.

All likely emergency conditions should be identified with the full involvement of employees. Such conditions may arise, for example, from severe natural events (high winds, floods, seismic and volcanic activity), or equipment failure or structural collapse, or loss of containment of hazardous substances. An emergency co-ordinator should be appointed in advance to take control in any emergency, and the actions established that should be undertaken in the event of specific cases occurring, such as a chemical spill. Back-up systems for light, power and telecommunications may need to be provided. Alarm signals, where appropriate, need to be established and means of communication identified. The plan should specify which emergency services need notifying in any given case, and by whom. Procedures to account for all people on site, including visitors, need to be put in place; search-and rescue plans determined; and shut-down procedures for processes, plant and machinery worked out.

In the event of a major emergency, a nominated person should be responsible for the release of information to the media and the public. There should be a pre-arranged means of giving an all-clear signal, with re-entry procedures and plans developed to enable a speedy return to normal operations as soon as possible.

The emergency plans should be reviewed periodically (at least once a year) by management with the involvement of employees. As part of this review, it would be considered whether the plans meet the objectives set earlier, the practice drills have revealed any deficiencies and whether the emergency services are satisfied with the arrangements.

High Hazard-Potential Worksites

On large sites where there is a high hazard potential, inadequate risk management and the lack of appropriate emergency procedures should things go wrong can lead to far-reaching consequences. The incident described in Case Study 8.2 led to an inquiry by an Australian Royal Commission, which called for major changes in the regulation of facilities with a high hazard potential. The Commission's main recommendation was that the operating company must undertake a safety case or report approval under the Australian National Code for the Control of Major Hazardous Facilities 1996, to identify, monitor, audit and review safety systems against Australian and international standards. Operating standards would need to be reviewed periodically, including start-up, shut-

Case Study 8.3 The Longford Gas Explosion

On 25 September 1998, a series of massive explosions and fires destroyed much of the gas-treatment facility at Longford, Victoria, which supplies natural gas to the State's grid, and gases including liquefied petroleum gas (LPG) to Long Island. The explosions continued for over an hour, and the fires for 53 hours, with the result the most of the State of Victoria went without gas and hot water for two weeks.

Difficulties in getting a circulating pump for warm lean oil to work led to a sudden pressure surge, which caused a weld failure on a very cold heat exchanger, releasing 10 tonnes of gas and oil in a matters of seconds. This exchanger had been operating for some time with broken tubes, which was causing process difficulties in other parts of the plant. The escaping hydrocarbons formed a large vapour cloud, which ignited on reaching gas-fired heaters still working some 130m away. The vapour cloud burnt back rapidly, igniting the original source of the emission, which led to a sequence of further explosions and prolonged fires.

The Commission's Report recommended that the site's training procedures should be improved so that all plant operators can readily understand the plant's hazards and process operations, and that such training must be able to assess the operators' ability to retain information taught. The Commission also recommended that an incident-reporting procedure be introduced, not only when injury or damage occurs, but also for process upsets, which may lead to useful knowledge of the plant's operational behaviour. The Company owning the site should be required to show that adequate operating and maintenance expertise is on site at all times, and operating practices are reviewed periodically. It must dedicate an office with a manager in charge of the safe operation of the plant.

Although the Commission did not comment on the safety implications of production pressures, these may have been a factor that led to the various maintenance deficiencies noted in their Report. *For processes that cannot be readily shut down without causing substantial disruption to output affecting numerous customers, there is strong pressure from senior management to keep the plant going and tolerate apparently minor malfunctions*. Moreover, pressure on operators had increased by management's decision to relocate all professional engineering staff to Melbourne, with shift-supervisor responsibilities reallocated to operators, and supervisors downgraded. *Between 1993 and 1998, the number of supervisors had been reduced by one-third, and maintenance staff cut from 67 to 58*. The Australian newspaper, *The Age*, reported a staff survey carried out before the blast revealed concerns about overwork affecting safety. Plant drawings had not been kept up-to-date and did not show a number of plant modifications made after start-up.

Clearly these various management decisions had cumulatively increased the chance of a minor mishap escalating into a major disaster, with the lack of adequate training and an insufficiency of supervision.

down and emergency shut-down procedures, as well as deviations from normal working conditions. A fire-risk analysis and emergency-response plan should also be made.

At the time of writing this book (late 1999), the Victorian WorkCover Authority

(VCA) is proceeding to draft regulations for the control of facilities of high hazard potential, with the setting-up of a major hazards unit. In New Zealand, a similar unit foreshadowed under legislation has yet to be formed.

Accident Reporting

The Department of Labour has for a number of years received notification of accidents occurring in places of work. This information has been used to monitor compliance with regulations and establish a database to determine trends in occupational safety.

Under the Health and Safety in Employment Act 1992, employers are required to keep a register of *all accidents where someone was or might have been harmed*. Where serious harm has occurred, an employer must notify the Occupational Health and Safety (OSH) Service as soon as possible after its occurrence. In some industries of high hazard potential, the Service must be notified whether or not serious harm has happened.

Whenever there has been an accident involving serious harm to any person, no-one may alter the scene of the accident without the permission of an OSH inspector. There are certain exceptions to this rule, including:

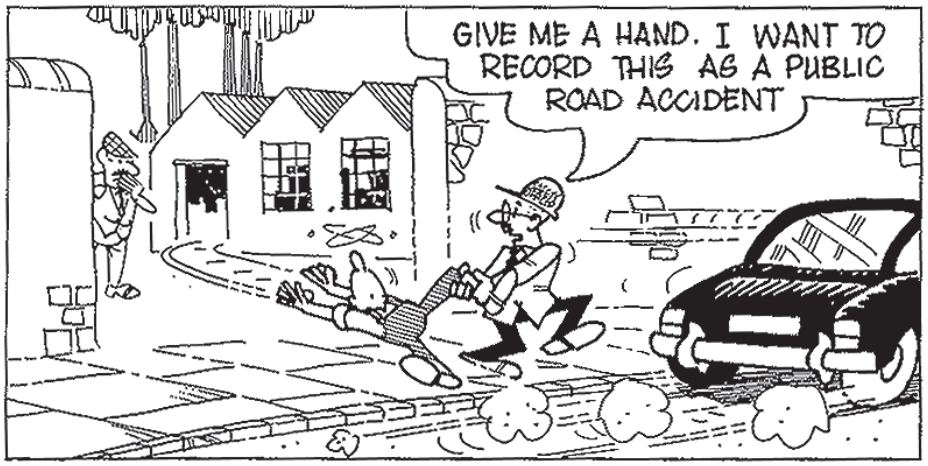
- the need to save life and prevent further harm and suffering;
- to prevent serious damage or loss of property; and
- where the accident involves a motor vehicle on a public highway.

The reporting of accidents, including so-called "near-misses", leads to the identification and thus elimination or control of dangerous situations and work practices that also affect production and quality of work. The literature on accidents backs up the need to report all incidents. Minor accidents and near-misses provide hazard warnings of more serious incidents. If these smaller failures can be controlled, then the larger ones will be controlled in turn. *Prevention is better than cure*.

The record of failures and unreliability also provides a database to evaluate the risk of new ventures. For example, the likely safety levels of the then (early 1980s) proposed nationwide scheme for storing and transporting LPG in bulk was estimated on the basis of historic data gleaned from experience in the petroleum and other industries.

Reference

1 Lardner, R, Miles, R and Flemming, M (2000): "Safer behaviour at work", *Chem. Eng.*, No. 694, 23.



9 Legal Responsibilities

From the earliest of times, the law has taken a magisterial interest in accidents and those who cause them. Legislation has been enacted to prescribe ways of avoiding such mishaps. Bond[1] notes that the Code of Hammurabi (1700 BC) laid down a duty of care for builders:

> *No. 229. If a builder builds a house for a man and do not make its construction firm and the house he has built collapse and cause the death of the owner of the house - that builder will be put to death.*

Bond comments that the effect of this legislation on the accident rate is not recorded, but he assumes that it must have jolted senior management into looking at fresh work practices in the building industry of the times!

In medieval English law, any chattel that caused death was forfeit, and had to be offered to God as a deodand (*deo dandum*, gift to God). The last time it was invoked was in 1841 at a coroner's inquest inquiring into the deaths of eight passengers on a train that had ploughed into a mound of earth dislodged from an excavated cutting after heavy rain. The jury declared a deodand of one thousand pounds on the unfortunate railway engine, payable to the Lord of the Manor where the accident happened.

Development of Industrial Safety Law

New Zealand Law is based on English Common Law, and health and safety legislation has often tracked British developments. These may be seen as a continuous regulatory process over the past 200 years to mitigate and control the adverse impacts of industrial activity. The appalling working conditions of children in some of the Lancashire cotton-mills led to the first Factories Act, the Health and Morals of Apprentices Act 1802. This was followed by a succession of acts which regulated workplace and technical hazards. In 1863, the Alkali Act was passed to control the emissions from chemical factories supplying bleaches, detergents and dyestuffs to the textile industry. This legislation set up an Alkali Inspectorate, the forerunner of the present-day Health and Safety Executive. The growth of law over the years led to fragmentation, with five separate Government departments, various local authorities and seven separate inspectorates involved by the mid-twentieth century. Further, the Law could not keep pace with technological change. Robens[2], in a far-reaching inquiry on health and safety at work, recommended sweeping changes: there should be a more unified framework of control based on better self-regulation, with both

employees and employers having responsibility for safety.

At that time, New Zealand had its own mosaic of safety law including: the Machinery Act 1950, the Construction Act 1959, the Explosives Act 1957, the Dangerous Goods Act 1974, the Boilers, Lifts and Cranes Act 1950 (a historical collection of legislative requirements from the days of steamship travel), the Electricity Act 1968 (and the subsequent wiring and supply regulations), the Health Act 1956, the Poisons Act 1960 and the Radiation Protection Act 1965. New ventures could fall under the provisions of the Town and Country Planning Act 1953.

A review of this disconnected set of New Zealand legislation and corresponding number of statutory agencies to administer it, often without the need to consult with each other, led Walker[3] to propose a somewhat similar philosophy to that recommended by Robens in the United Kingdom. The Government responded cautiously: after various methods of co-ordination were tried out, the Health and Safety in Employment Act was passed in 1992, to become effective from 1 April 1993, nearly twenty years after the equivalent statute had been passed in Britain.

However, the various building regulations had already been revised in a new Building Act 1991 and its Regulations 1992, which were outcome-driven, rather than prescriptive of the methods to achieve satisfactory performance. It introduced the requirement of a warrant of fitness for a public building, a concept that echoes the requirement under the Consumer Act that an article must be fit for its specified purpose. Moreover, the Health and Safety Act was seen to be subservient to the overarching provisions of the earlier Resource Management Act 1991 with its demands that effects must be eliminated if possible, and if not eliminated, mitigated or reduced. "Effects", in this context, covered adverse impacts of all kinds, whether of short or long duration, whether infrequent but major in consequence, or frequent but of lesser magnitude. Resource consents would progressively replace the older permits for emissions to air and discharges to waterways.

The latest element in the new legislative order was the passing of the Hazardous Substances and New Organisms Act 1996 to protect the environment and public health and safety by managing the adverse effects of dangerous substances including those of biological origin. Under this Act, an Environmental Risk Management Authority was set up in 1998 to decide whether hazardous substances and new organisms should be introduced into New Zealand and, if so, under what conditions.

Duty of Care

MacKenzie[4], in reviewing the legal responsibilities of engineers, notes that the

Law imposes on everyone an obligation to practice her or his profession with a proper degree of care and skill. He quotes a judgement from the last century (*Badgley v. Dickson, 1886*):

> *"As an architect, he is in the same position as any other professional or skilled person, and whether it be in the preparation of professional plans and specifications, or the doing of any other professional work for reward, is responsible if he omits to do it with an ordinary and reasonable degree of care and skill."*

To determine what is a reasonable degree of care and skill, one has to compare what is usual and customary for a fellow professional person to know and do under the same circumstances. Failure to comply with generally accepted practice, and the use of codes if applicable, may be taken to imply negligence. MacKenzie[4] quotes another judgement to illustrate this point (*Bevan v. Blackhall & Struthers, 1973*):

> *"I am of the view that bearing in mind the function of codes, a design which departs substantially from them is prima facie a faulty design, unless it can be demonstrated that it conforms to accepted engineering practice by rational analysis."*

With less prescriptive legislation than hitherto, the defence of rational analysis would seem to take on greater importance.

The general standards and practice of the profession are not the sole test of the standard of care. The general practice of the profession may be deemed to be inadequate; that is, the Court may determine that the general practice of the profession does not meet the test of what a reasonable and prudent person would do. In such a case, the Court may maintain that there has been negligence, even when usual engineering practice has been observed.

The exact standard of care imposed by the Law will be affected by the degree of expertise in the particular field that the engineer claims to have. If an engineer claims expertise in structural engineering, for example, that person will be judged by the general standard of competence of structural engineers. Thus it is important for engineers in their work to make others aware of areas in which they are not competent, as well as informing them of areas of expertise.

In design, an engineer would normally be held responsible for any technical defects. However, an engineer may be required by an employer or client to use an untried method or new technology to meet particular schedule or cost criteria. MacKenzie[4] advises that the proper course for an engineer, where there is a choice between a design which conforms with conventional codes and technology and another which is untried and cheaper and holds risks, is to advise the employer or client of the greater risk, and leave the commercial decision to

that person. It is the employer or client, not the engineer, who will gain the commercial benefit. Nevertheless, if the risk is too great, then the engineer may be under a moral duty to others to ensure that the high-risk option is not taken.

This moral imperative would also seem to apply to subcontractors. The public good should hold precedence over the contractor's obligation to build to a specification should this be perceived to be faulty. It is within the realm of competence of both the client and the contractor to seek alternative lower-risk designs.

When a design includes the likely cost of the work within a specified timeframe, it is normally an implied condition that the project should be capable of being completed within a reasonable range of those estimates. The engineer is responsible for any lack of care in preparing these. In the case of construction work, an engineer may be required to make reasonable enquires regarding the solvency and capability of any firm submitting a tender, and so advise an employer, although it is not expected that any guarantee can be provided. In preparing any contract, the engineer is usually required to ensure that the specifications are drawn with sufficient clarity, and the general conditions of contract are appropriate. The engineer is also under a duty of care to see that all necessary drawings and instructions are given to a contractor within a reasonable time.

As far as supervision of contracts for civil engineering work is concerned, the engineer must properly supervise the works and inspect sufficiently frequently to ensure that the materials and workmanship conform to the contract. While the engineer cannot be expected to be on site all the time, there are normally critical phases in the work when the supervisory duty can only be undertaken by a personal visit. In general, the duty of the engineer is to be able to certify that the work has been carried out according to the contract, particularly in respect of progress payments.

In the case of supervision of other work, such as the fabrication of process plants or the assembly of machines, the design engineer is expected to have frequent interaction with workshop staff or contractors involved in the manufacture to ensure that the design intentions are carried out. Often, with complex or novel work, the design engineer will be asked to interpret his or her intentions, with further instructions to carry out the work, and this discussion may lead to the consideration of alternatives or substitution of components. The design engineer will not normally be liable for such changes if these were made in good faith with sound engineering judgement.

Legal Liability

An engineer's failure to fulfil the standard and care required by law may fall

under either of two legal heads of liability:

1. *Contract*. The duty to exercise the requisite duty of care to the client arises from the terms of the contract, expressed or implied, between the engineer and the client. The exact extent of that obligation owed will be interpreted in the light of that contract.

2. *Tort*. The responsibility of an engineer to a client is not the sole one. The engineer may also be liable to third parties with whom he has no contract. The basis of this liability in law is tort of negligence, which happens when a person commits a negligent act or omission, thereby causing harm to another person whom the negligent person ought reasonably to have contemplated as being likely to be affected by that act or omission.

A professional engineer is negligent if he or she fails to observe the standards of a prudent fellow professional person. So, the standard of care in negligence is similar to that owed in contract, but it is owed to the world at large, and without the benefit of any particular limitation or exception which may be contained in the contract.

An extension of liability in tort to third parties has arisen as a result of a particular case, *Hedley Byrne v. Heller & Partners (1963)*. That case established that there can be liability for negligent statements, as distinct from negligent acts or omissions. This has an important effect, so far as engineers are concerned, in extending possible liability. An example might be where an engineer is required to furnish some kind of certificate of performance or warranty which, if negligently given, would render the engineer liable should any loss be incurred as a result of reliance being placed on the certificate.

The fact that liability in tort runs alongside liability in contract has some important consequences. While a consulting engineer may have, in his contract with his client, specifically limited the degree of responsibility that he or she is undertaking, that limitation may not apply to third parties. Woodhouse, in a judgement in the case, *Bowen v. Paramount Builders Ltd 1977*, said:

> *"I do not regard a private contractual arrangement for an inefficient design or for an unworkmanlike or inadequate type of construction as any sort of 'justification or valid explanation' for releasing the builder from his duty to those who otherwise could look to him for relief."*

Woodhouse's comment reflects the blunt observation of Pavolic[5]:

> *"If an engineer is troubled because he believes that the product that he is working on poses a threat to the public health, safety, and welfare, he does not need to be told that he is to hold paramount public health, safety, and welfare."*

If applied to consulting engineering practice, this ruling would mean that, even if an engineer had specifically limited the extent of reliability to the client, because the client was not prepared, for example to pay to have the job done as thoroughly as might be required, *the engineer might still be liable in tort for any damage suffered by other persons whom he or she ought to have contemplated as being likely to be affected.*

There is another consequence of the distinction between tort and contract. Under the Limitation Act 1950, the law provides that any claim, in contract or in tort, must be brought within six years from the time when the cause of action arose. However, there is a distinction between contract and tort regarding when the cause of action arises. A cause of action in contract arises as soon as there is a breach of the duty of skill, whether or not any damage has been apparent. A cause of action in tort arises only when there is both a breach of the duty of skill and damage. Accordingly, where there is negligence, but its effects do not become manifest for some years, claims in tort will not be barred by statute until six years after the damage has become apparent. In the case of deficient building work, a case was argued through to the House of Lords, who ruled in 1983 that a cause of action in tort for negligence in the design and workmanship accrued at the date when the physical damage occurred, whether or not the damage could have been discovered with reasonable diligence at that date. In New Zealand, it is also important to note the "long-stop" provision contained in Section 91(2) of the Building Act 1991, which prevents civil proceedings that relate to any building work being brought against any person ten years or more after the date of the act or omission on which the proceedings are based.

Limitation of Liability

There are two ways in which self-employed and consulting engineers may be able to limit their liability for professional negligence. These are by inserting suitable terms in the contract of engagement and through the formation of a limited liability company.

1 Contract terms

It is possible to define, by appropriate terms in the contract, the liability of the parties for a breach of that contract. Common Law generally recognises the principle of freedom of parties to strike contracts on such terms as they wish, and there is no general rule of law by which Courts can refuse to give effect to exclusion clauses. However, the Courts have, where appropriate, applied a number of general rules in the law of contract in such a way as to control the possibilities of abuse which are inherent in having complete freedom of contract in setting exclusion clauses.

MacKenzie[4] notes, in particular:

- Anyone seeking to rely on an exclusion clause must show that it was incorporated in a term of the contract, and that reasonable steps were taken to bring the clause to the notice of the other party at the time the contract was being drawn up.
- An exclusion clause is to be construed strictly against the party who introduced it and seeks to rely on it.
- The exclusion clause will be binding only upon the parties to the contract and will not offer protection against claims by third parties; moreover, it may not protect others who have been engaged by the engineer and who sought the limitation of liability.

2 Limited liability company

An engineering consultancy may limit its total liability for a claim by incorporating the firm as a limited liability company. If a judgement is made against the firm, then the total amount of the firm's liability will be the assets of the company. However, the limitation of liability does not protect individuals who have been negligent, against whom an action for liability in tort can still be brought.

For this reason, it is normal practice for consulting engineers, and a condition of membership of their professional association in New Zealand, to take out professional indemnity insurance against claims. As with all insurance, the purpose is to spread the risk of calamity among many to avoid ruinous loss for the individual. Risk insurance is considered further in Chapter 10, including legislation that affects insurance in New Zealand.

Standards and Compliance

Standards represent widely recognised benchmarks of industrial safety and performance, and thus a means of managing risk. Although the use of appropriate Standards in engineering work is prudent, and is normally regarded as "best practice", only a very small proportion of published Standards (approximately 5%) are mandatory. At a national level, Standards become mandatory when they are incorporated into specific acts or regulations. Local authorities, such as city and district councils, can create bylaws, which incorporate standards, such as NZS9201: *Model general bylaws*.

For the construction industry, the Building Act 1991 and the Building Regulations provide the framework for legal compliance. The regulations contain the *New Zealand Building Code*, which sets minimum standards for building work. To meet the requirements under this Code, the Building Industry Authority provides prescriptive *Approved Documents* of two kinds: acceptable solutions and verification methods. Both types of document may refer to specific Standards.

Standard conditions of contract for building and construction may be found in NZS3910:1998 *Conditions of contract for building and civil engineering construction*. The Standard provides a mechanism for resolving disputes, which might otherwise have ended up in court, to be resolved. NZS:3910 has provisions that require any dispute, which cannot be resolved by agreement between the two parties, to be resolved by mediation, if both parties agree, or otherwise determined by arbitration.

At the time of writing (1999), only four standards that relate to product safety are cited in legislation under Section 29 of the Fair Trading Act. These concern products for children and cigarette lighters, rather than engineering appliances.

Disputes that come before the courts may use Standards as evidence. For example, in 1998, the Environment Court in Christchurch rejected a school's appeal against a cellphone tower being built next to the school, drawing on an interim radiofrequency standard, now NZS2772:Part 1:1999, *Radiofrequency fields - maximum levels*, to support its decision.

Statutory Obligations

Resource Management Act 1991

Under Section 17 of this Act, there is a general duty on every person to avoid, remedy or mitigate any adverse effect on the environment arising from any activity carried on by, or on behalf of that person, whether or not permitted by a plan or by a resource consent or existing rights. The meaning of "effect" in the Act is very broad. It covers any past, present or future effect and any cumulative effect which arises over time in combination with other effects regardless of scale, intensity, duration, or frequency of the effect, and also includes any potential effect of high probability as well as one of low probability which has a high potential impact. Clearly, much engineering activity has an effect in these terms.

The provisions of the Act can unwittingly expose an engineer to unforeseen legal risks. For example, an engineer may decide, as a matter of urgency, that certain emergency work is needed on a building site to stabilise a landslip which was threatening to overwhelm the construction. He might order that a retaining wall be built at once to stem the hazard. Such work, however, would be a violation of the Act insofar that no resource consent had been obtained for the emergency work. While the engineer might have a defence, if it could be argued that there was risk to life and limb, the legal exposure remains.

Another example of exposure under the Act is provided by the failure of the Opuha Dam while under construction, which resulted in a considerable amount of debris being borne downstream in a flood of water. The dam builders and the project manager were charged under the Act with the unlawful discharge of

contaminants. Case Study 9.1 gives a more detailed account of the circumstances and court proceedings.

Case Study 9.1 The Opuha Dam Collapse (taken from newspaper reports)

An earth dam was being erected on the Opuha River, South Canterbury, to enable the surrounding area to be irrigated and with some electricity generation. On 6 February 1997 (Waitangi Day - appropriately named weeping waters), following a severe rainstorm, the almost-completed dam collapsed unleashing a major flood of about 13 million cubic metres of water and about 200 000 cubic metres of silt, gravel and rocks. Recorded river flows at Skipton bridge rose eightfold in a day before the measuring station was swept away. The bed of the river at this bridge was estimated to have been raised permanently by 1m. Farmland for several kilometres downstream was devastated, and almost all fish and insect life on the river was killed. One farmer lost 257 sheep and had to replace 8 km of fences. Repairs to the river's flood-protection system cost almost $600,000.

Subsequently, Canterbury Regional Council prosecuted the dam builders and the project manager in the Environment Court for allowing the unauthorised discharge of contaminants, the water and the earth-dam construction material, into the river. The builders, it was said, were required by their insurers to build the dam in such a way that it could withstand a one in ten-year flood during construction. In October of the previous year, so that they could use the full width of the dam for filling purposes, the builders had diverted the river though a 1.8-m diameter pipe which, it was claimed, could not cope with a one in ten-year flood. During this period, the estimated height at which the dam was considered to be capable of holding back such a flood, as advised by the builders' consulting engineers, was reduced by 5m. This lower estimate implied a reduction in the dam's flood capacity of some 3.2 million cubic metres.

When heavy rain at the beginning of February 1997 overwhelmed the pipe and caused water to accumulate behind the dam, there was no specially-formed channel which could be unplugged to help take the increased flow of water. On 5 February, the project manager arranged for bulldozers to create a channel on the side of the dam to release the accumulating water. The water going through this new channel began to scour the downstream face of the dam, which was not designed to cope with the swirling mass of water. Eventually, a major break in the dam occurred, causing a huge release of water and debris downstream.

The Court was told that it was not necessary to prove either intent or negligence on the part of defendants who would assert that their actions were necessary to prevent serious damage to the dam structure and to properties downstream. Defence lawyers argued that the dam had been built in compliance with the resource consents, and this state of affairs had been certified in a letter from the Council's chief executive officer during the construction as a result of monitoring the work.

The Court found that an illegal discharge had taken place which made the defendants liable to a $200 000 fine and/or a two-year term of imprisonment. In his reserved judgment, the judge said that there had been an intention to leave a 10m-wide channel in case of flooding during construction, but when such a channel was needed, there was none. Both defendants knew that the dam could be overtopped in the event of a flood, but took no reasonable steps to prevent it: that made the defendants responsible for causing the collapse of the dam construction material into the river when they dug an emergency channel in the dam face to prevent floodwaters overtopping it.

The case went to Appeal, on the grounds that the judge had made an error in regarding the loss of material as a "discharge". The High Court, however, found that the judge was

entitled to construe the loss of the dam's material as a discharge, provided the appellants could be causatively linked to it. "We have no difficulty with the notion that where an earth dam is under construction, those responsible for it must ensure that the dam materials are not at risk of being washed away, as happened here," the appeal judges concluded. The Appeal was dismissed.

This judgement is an important decision, since the defendants had not deliberately set out to circumvent the law and had acted under engineering advice. It is also important since the action was taken in terms of a breach of environmental law under the Resource Management Act rather than one of tort for negligence.

Health and Safety in Employment Act 1992

As noted in Chapter 8, this Act places a duty of care on all employers to ensure the safety and health of their employees. Sections 7 and 10 of the Act set out in detail the steps an employer must take to provide a safe working environment. Employers must identify hazards in their place of work, and regularly review them to see if they are significant and require further action to control them. Whenever an accident or serious harm occurs, an employer must register it on a prescribed form. An employer must ensure that employees are sufficiently trained to do their work safely or supervised by an experienced person. Moreover, an employer is responsible for ensuring that an employee does not harm any other person while at work, including members of the public and visitors.

Since effective safety management requires the involvement of everyone in a workplace, employees also have responsibilities to look after themselves. For example, if an operator removed a machine guard to give better access to the machine (as described in Case Study 8.1), despite the best intentions of the employer, both the employer and employee would share liability. However, if the employer could show that all practical steps had been taken to comply with the Act, the employer might be found innocent.

Under Section 16 of the Act, any person, even if not the employer, who controls a place of work, has the responsibility for ensuring that people in or near the workplace are not harmed. Likewise, self-employed people must ensure their action, or inaction, does not harm anyone, including themselves. Any principal, a person or company who hires any contractor or subcontractor, must take all practicable steps to ensure that they or their employees are not harmed at work.

That there is a duty owed by principals to their contractors has been confirmed in a decision of the Court of Appeal in the case of *Central Cranes Limited vs Department of Labour 1997*. While a principal may promote the safety of his

or her employees, the obligations to a contractor called to a workplace to undertake various tasks must also be considered. The principal cannot assume that, if a person is employed by another company, then the responsibility for health and safety rests solely on the shoulders of the employer. The issue before the Appeal Court is summarised in Case Study 9.2.

Case Study 9.2 Principal's Liability

A principal had been prosecuted under the Act in the case where a contractor's employee had been seen working 41m above a construction site without a helmet or protective harness. The principal argued that it was the worker's employer, not the principal, who should be responsible for the safety of the worker. The Court of Appeal rejected this argument by finding that, although the responsibility rests primarily with the employer, the principal's own responsibilities in securing a safe workplace are not thereby diminished. Moreover, the Court observed that under the Act a principal is required to take all practicable steps to ensure workplace safety. A principal cannot distance him or herself from what is happening in a workplace simply because contractors are involved who, in turn, have a more direct responsibility towards their own employees.

Thus a principal must put in place appropriate procedures to ensure that contractors and subcontractors are meeting their obligations to their employees who are working onsite. In the engagement of a contractor or subcontractor, a principal is advised to make it a term of the contract that the contractor complies with the principal's health and safety policies and codes of practice as well as the contractor's own policies and codes.

The Act specifies two kinds of offences. The first and more serious kind relates to an action or inaction taken despite the knowledge that death or serious harm is likely to be caused thereby and the action or inaction is contrary to a provision of the Act. The second kind relates to failure to comply with the provisions of the Act, or regulations under the Act. A person, if convicted of the first kind of offence, could be fined up to $100 000 or face up to one year in prison or both. Offences of the second kind could result in penalties up to $50 000.

Consultation

Although it is prudent to be open with neighbouring parties about proposed developments, there are a number of instances where notification or consultation is a legal requirement. Such a requirement does not, however, imply a requirement to gain unanimous consent.

The requirement to notify or consult may be set out directly, as in the Resource Management Act 1991. It may also be imposed by case law as, for example, the Court of Appeal had held that consultation by Crown agencies with Maori to be a recognised principle of the Treaty of Waitangi. In addition, there are a number of statutes that require the principles of the Treaty to be taken into

account, such as the Resource Management Act 1991 and the Hazardous Substances and New Organisms Act 1996.

Watson[6] lists six criteria that the Court of Appeal has recognised in respect of the duty to consult:

- Meetings must be held with parties who are required to be consulted;
- Parties must be provided with relevant information;
- Parties must be provided with further information if requested;
- The meetings must be entered with an open mind;
- Due notice must be taken of what was said at such meetings;
- Parties must have their say before a decision is made.

The Planning Tribunal noted in the case, *Ngati Kahu v. Tauranga District Council*, that the Council could not be bound to consult for as long as it took to reach consensus. The Council was obliged to consult for a reasonable time in the spirit of goodwill and open-mindedness, enabling all reasonable options to be considered carefully and explored. In determining whether appropriate consultation has taken place, the Planning Tribunal emphasised that consultation is a two-way process, with each party having a responsibility to work in good faith. If such consultation has taken place, and despite efforts to find a mutually acceptable solution there is still disagreement, then this situation must be accepted as the outcome. The Council was free to make the decision it did, having fully met its obligation to consult.

Although the legal answer is that the courts will uphold the validity of such a decision, and the project from a legal viewpoint may go ahead, a project may founder, however, because of objectors' other tactics, such as withholding access to land. The hardest part of any major engineering project is not the technical solution but the gaining of public support. If people have been invited to give their opinions and be listened to, then they are much less likely to obstruct the final decision even if they disagree with it.

Registration of Professional Engineers

Newnham[7], on reviewing engineering history in New Zealand, noted that statutory registration of engineers arose out of a concern for competency in work undertaken by persons, who called themselves "engineers", for which work they were unfitted. This concern emphasised the need for a proper system of education and training for professional engineers and the desirability of registration of engineers, or some other form of control, so that persons requiring the services of professional engineers could be reasonably sure that the engineers

were properly qualified to carry out the work for which they had been engaged.

In various Australian States by 1920, legislation had been in place for several years requiring local authority engineers to be properly qualified. The New Zealand Society of Civil Engineers (the forerunner of IPENZ) presented a bill to the Government of the day based on the 1911 Queensland Act. Because of conflicting views, a revised bill did not become law until 1924. From 1946 onwards, corporate membership of the New Zealand Institution of Engineers (now IPENZ) was accepted as a recognised qualifications certificate for the purpose of registration.

The Engineers Registration Act 1924, amended in 1944, is still in force in 1999. The essential purpose of the Act is the requirement that engineers with control of expediture of public money be registered (with certain minor exceptions). However, for some time there has been a measure of disquiet that this Act now only covers a section of the Profession. Whereas in 1920 most engineers were employed in government or local body service, some seventy-five years later a majority were employed elsewhere. In 1994, the then Minister of Commerce wrote to the Engineers Registration Board formally to ask whether the 1924 Act should be replaced or done away with altogether. The Board consulted widely, seeking views from registered engineers, professional institutions such as IPENZ, ACENZ (consulting engineers) and ALGENZ (local government engineers) and the Consumers' Institute. It also looked at the experiences of the Medical Council and the Society of Accountants. The general agreement was that a register is still needed, but will have to be a considerably tighter arrangement than the one now currently operated. Registration Certificates should reflect a knowledge of relevant New Zealand codes, while all engineers need to demonstrate ongoing competence to maintain their registered status. By operating a system of identifying professional engineers who have met certain minimum standards, the community would be given a level of protection from the outset of any engineering work, since engineering failures impact heavily on the health and safety of the community. At the time of writing (1999), draft legislation is being prepared to give effect to these ideas.

Some engineers in New Zealand have sought and gained recognition from overseas authorities, such as the Engineering Council of the United Kingdom, which grants Chartered Engineer status to engineers by virtue of approved academic qualification, training and experience.

References

1 Bond, J (1996): *"The Hazards of Life and All That",* Inst. Physics, Bristol.

2 Robens, Lord (1972): *"Safety and Health at Work",* Cmnd 5034, HMSO, London.

3 Walker, I K (1981): *"Occupational Safety",* State Services Commission, Wellington.

4 MacKenzie, A D (1984): "The legal responsibility of engineers", in *"Engineering Risk",* 71-83*,* IPENZ, Wellington.

5 Pavolic, K. (1983): "Autonomy and obligation: is there an engineering ethic", in Schaub, J H and Pavolic, K ed., *"Engineering Professionalism and Ethics",* Wiley, New York, 223-232.

6 Watson, J (1998): "Consultation - law & possibility", *N.Z. Eng., 53*/5, 7-8.

7 Newnham, W L (1971): "*Learning Service Achievement. Fifty Years of Engineering in New Zealand"*, NZIE, Wellington.

10 Risk Insurance*

Insurance is a form of risk transfer. It does not alter the technical risk in any way, but eases the financial risk by distributing the loss among others in the community. Insurance is inherently a risk-sharing tool for the community, with the insurers in the market acting as the funding mechanism for the pooling of such risks.

In effect, insured parties gain access to the pooled funds of the insurers as an added security against those losses that when, or indeed if, they occur and they cannot adequately fund the loss for themselves.

It is a basic premise that the purchase of insurance for most risks, apart from the major ones, is a financial transaction similar in form to a loan. The question that should always arise is: will the insurance be effective in reducing the total cost of risk more than other possible risk-management options?

All insurance contracts contain certain terms, conditions, exceptions and limitations and therefore *only cover what they are intended to cover.* There are certain risks for which insurers will make their resources and capital available but there are other risks they do not wish to contemplate, or alternatively will only accept under special conditions with limitations and restrictions.

An insurance policy will normally have an excess or deductible amount that the insured will pay in the event of any claim. This is a reasonable proposition as it involves a commonality of interest between the insurer and insured in sharing some of the risk. Above this amount the underwriters may provide a primary layer to provide the cover for a sum up to the maximum limit of indemnity available.

Risk Management and Insurance

The management of any capital project represents a challenge and risks which begin with the conceptual stages, continue through the life of the project and beyond completion during future permanent occupation.

It does require the co-ordination of a wide range of skills and disciplines to ensure the risk issues are properly identified, measured, managed and financed.

Too often the traditional approach has simply been to address the design, construction and observation issues and risks by the utilisation of standard conditions of contract, arrange some fairly standardised insurance contracts; then to trust that the project will be completed satisfactorily.

*** based on text provided by Don Houchen**

In fact, an integrated approach is essential having regard for not only the design, construction and supervisory functions and risks but also an appropriate specification needed for the insurances of those risks which can reasonably be insured.

Risk management practice makes extremely good sense whatever insurance regime may ultimately be in place. *Not all of the project risks can be catered for by insurance and it should never be regarded as a substitute for an adequate risk management programme*.

As discussed earlier in this book, the **first stage** in the risk-management process is *to identify and measure the risks* and having done so, to examine them and the ways and means of avoiding, reducing or minimising them.

The task of formulating a programme for managing the risk should be viewed as the minimisation of the total cost of risk coupled with an assessment of alternative risk-financing methods.

Self-funded programmes which require a major contribution from the participants themselves in the event of a major disaster present a real problem. In many instances, it is often a better strategy to place the individual risks in the insurance market.

There is the potential for failure in such a scenario. If a regime of self-insurance is under-funded, then the reality is that the participants themselves, having suffered significant losses, may be responsible for any shortfall.

The **next stage** in the process is *risk control*. Risk control is the active management of and monitoring of risks in order to minimise their frequency or severity. As noted before, it facilitates the most appropriate means of funding the risk and *may even reduce the cost of insurance*.

The **final option** is *risk transfer*. The means by which risks can be regulated or transferred appropriately are by way of suitable provisions in contracts. There are recognised standard documents that can appropriately regulate and share the responsibilities between the parties involved in various activities, in particular construction projects.

In any capital project it should be recognised no project can be successfully completed without the various parties assuming their proper share of the responsibilities and risks.

Simply shifting responsibilities and risks from one party to another, which the other party or parties are not qualified to assume, or are not financially able to accept or can even insure, can be a fruitless exercise.

From a financial point of view, one of the important aspects of risk transfer will be the arranging of the insurance programme. The cost of insurance for a project

may be significant, but a major part of this cost may not be identifiable at the outset.

Insurability

The process of dealing with the selection and pricing of insurance risks is commonly known as *underwriting*.

The acceptability of a risk to an underwriter depends upon the presence of a number of criteria to ensure the viability of the insurance contract. The item to be insured may be a thing or an activity. Hammond[2] lists these criteria as follows:

1 *A large number of similar items exposed to loss*. This criterion provides a database from which the risk can be evaluated and a premium set.

2 *A loss definite in time and place*. The estimate of risk and settlement of a claim are greatly enhanced if the time and place of the loss-making event can be identified; it would be difficult to arrange insurance for the slow physical deterioration of a building, for example.

3 *Accidental loss*. A highly likely loss is not attractive, as the economics of insurance are based on the principle of risk-spreading among others the costs of random events beyond the normal control of the insured. Insurance may be more difficult and normally more expensive to arrange after a substantial loss.

4 *Minimal catastrophic hazard*. Catastrophes can produce instabilities in the insurance market, and financial ruin of particular underwriters.

Ultimately, insurability involves both actuarial and other business factors. As Hammond[2] notes, the actuarial factors of homogeneity, large numbers, definite and accidental losses and minimal catastrophic hazard are seldom met perfectly; one or more of them are likely to be compromised in establishing an underwriting decision for a client.

Insurance Classes

The number of policies that could apply to a construction contract, or indeed permanent insurance, are quite considerable. The various broad categories of insurance are listed by Adam[1] in the IPENZ publication *Engineering Risk* as marine insurance, material damage insurance, liability insurances and insurances of the person. These categories can be expanded as follows:

- *Material Damage insurance*.
- *Business Interruption insurance* against loss of production and profits.
- *Marine and Aviation Cargo insurance* against the perils of transportation.

- *Marine or Aviation insurance* for the vessels or craft and the legal liabilities to third parties arising from their use (including any charterers' liabilities).
- *General Liability insurance* in respect of legal liabilities that may be incurred to third parties for property damage and bodily injury.
- *Motor Vehicle insurance* in respect of vehicle damage and liabilities
- *Personal insurances*, such as life, accident and sickness insurance.
- *Professional Indemnity insurance* against claims regarding the competence of work or advice.
- *Directors' and Officers' insurance* to cover liability for wrongful acts in the management of the affairs of a corporate entity.
- *Statutory Liability insurance* to cover certain fines or penalties for inadvertent and unintentional breach of a range of statutes.
- *Employers Liability insurance* to cover common law claims by employees that fall outside of the scope of the Accident Insurance Act 1998.
- *Accident Compensation insurance* to cover accidental workplace bodily injury in terms of the Accident Insurance Act 1998 (note the Act was amended on 1 April 2000 by the introduction of the Accident Insurance (Transitional Provisions) Act 2000, with further reforms to be introduced by 1 July 2000).

Table 10.1 illustrates the number of policies that may be involved on a construction contract. (Note that this list is not necessarily exhaustive).

Alternative Risk Financing

Some alternative risk financing techniques have evolved to become the "standard" rather than the alternative for the risk managers of many major corporate entities and for many associations of entities who have bonded together to form *collective risk financing systems*. The essential elements are to cut insurance expenditure by retaining a greater degree of self-retained risk.

There is a wide range of self-funding concepts which can be considered:

- *simple self-insurance* by accepting higher levels of deductibles or excesses to reduce premium levels;
- *utilisation of accommodating insurers to provide claims administration services* for a negotiated fee;
- *more sophisticated structures* as employed by some professional associations and others who establish *risk management societies*, such as the Consulting Engineers Advancement Society Incorporated;

Table 10.1: A range of insurance policies that may apply to a construction contract

	Professional Liabilities	General Liabilities	Contract Works	Plant & Equipment	MV Third Party Liabilities	Employers Liabilities	Accident Compensation	Statutory Liabilities	Charterers Liabilities	Overseas Transit Risks	Advanced Profits
Principal	—	✔		—	✔	✔	✔	✔			✔
Project Manager	✔	✔	—	—	✔	✔	✔	✔			
Architect	✔	✔	—	—	✔	✔	✔	✔			
Quantity Surveyor	✔	✔	—	—	✔	✔	✔	✔			
Soil Engineers	✔	✔	—	—	✔	✔	✔	✔			
Specialist Consultants (other)	✔	✔	—	—	✔	✔	✔	✔			
Specialist Consultants Equipment	—	✔	—	✔	✔	✔	✔	✔			
Suppliers Materials	—	✔	—	—	✔	✔	✔	✔			
Contractor	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	

- *expansion of the degree of self-funding utilising the capacity of the group to retain risk,* facilitating the claims administration to be controlled and managed under collaborative agreements with accommodating Insurers;
- *the formation of captive or mutual insurance companies*, which may be categorised into national, international, limited membership, wider membership or professional or trade association related entities.

The cost advantage of economy of scale is often negligible in a disaster programme because it does require the accommodation of specialist insurers to complete such a programme.

The Nature of Insurance Contracts

A contract of insurance is inherently one whereby one party, *the insurer*, agrees in return for the consideration, the premium, to pay a sum of money or its equivalent to the other party, *the insured*, upon the occurrence of a specified event or contingency that affects an interest the insured has in the subject matter of the insurance.

The requirements follow the law of contract: and there must be binding agreement that complies with the general principles of contract law including an offer, acceptance and consideration. There must also be an "insurable interest"

with the object of the insured subject matter being a legal activity and not against the public interest.

However, these general principles are modified by a number of common law rules and through various provisions in the statutes that have special application to insurance contracts.

Most contracts generally are governed by the common law principle of *caveat emptor* "let the buyer beware". **This does not apply to an insurance contract**, which departs from this principle and it is a contract of *utmost good faith*.

The insurance contract has attached to it special obligations on one party "*the proposer*" to disclose certain material information that may not be fully available to the other party, "*the insurer*", when entering into the contract. *This requirement of utmost good faith forbids either party to conceal from the other any material thing which may have a bearing on the risk to be insured that is only privately known to them.*

This obligation is not confined to the insured. The insurer must also observe utmost good faith in dealings with the insured relative to the contract.

Co-insurance and Re-insurance

The insurance of larger risks is often undertaken by a combination of co-insurance and re-insurance. In *co-insurance*, the insurers take direct responsibility for providing a specified proportion of the cover, with the prime responsibility for assessing the risk being taken by a lead company. In *re-insurance*, the co-insurers lay off their risk with other insurers. For very large risks, the re-insurers may themselves re-insure further. In this way, such large risks are spread around financial institutions to minimise the individual impact of very large claims.

The availability of re-insurance can influence the insurability of an asset. Hammond[2] recounts an incident when a large commercial property, located below a dam, was declined insurance by a primary underwriter, largely because re-insurance was not available. Later, re-insurance capacity increased and became available to the underwriter who then accepted the risk.

The Classification of Insurance Contracts

One relatively simple method of classification of insurance contracts is into those that may be personal in nature; those that cover property losses; or alternatively those that cover losses arising from legal liabilities, depending upon the nature of interest insured:

- *Personal insurance* is concerned with covering the person or some other person for bodily injury, illness or death.

- *Property insurance* is concerned with the loss of, or damage to property.
- *Liability insurance* is concerned with losses arising from legal liabilities requiring the payment of compensation for damages to other parties.

A further distinction between various types of insurance contracts is between those *providing an indemnity*, as distinct from *those providing for other contingencies to be covered*.

The Principle of Indemnity

One of the controlling principles of insurance law for many insurance contracts is the principle of indemnity. According to this principle, the insured must be restored to a financial position that was enjoyed by him or her immediately prior to the event insured

This means, within the limits of the insurance, *the measure of the loss is also the measure of any payment by the insurer*.

The object of the principle of indemnity is to make certain the insured does not suffer financial loss, but may not make a profit from the insurance.

The Significance of Time of Claim

Most types of insurance contracts insure the consequences of accidental occurrences that take place during the currency of the policy.

Primarily, because *it is difficult to pinpoint an exact moment in time when a professional act, error or omission occurs*, Professional Indemnity, Directors & Officers, Statutory Liability and some other forms of liability insurance are underwritten on a basis of "Claims Made and Notified".

"Occurrence-based" policies

"Occurrence-based " policies of insurance, such as general liability insurance, are linked to a period in time. What is insured is loss resulting from a legal liability to pay compensation to a client or other third party that *has actually occurred during the period of the insurance*.

The simplest analogy for the application of an "occurrence-based" policy of liability insurance is a motor vehicle third-party liability insurance. If, for example, the insured negligently causes damage to a third party's motor vehicle at a time that fell within the period of the insurance, then any subsequent claim for damages by the affected third party *will fall to be indemnified by the insurer that provided the insurance cover at the time of the accident*.

This is the case, notwithstanding the fact that the plaintiff may notify the matter to the insured and then commences the action against the insured after the pe-

riod of the policy has elapsed. (There may be, of course, claim-reporting conditions in the policy that may affect any ultimate entitlement of the insured to the indemnity.)

"Claims Made & Notified" policy

Under a "Claims Made & Notified" policy of insurance, a different rule applies. *The policy responds only to those circumstances, of which the insured first becomes aware may lead to a claim or possible claim during its currency and then reports such circumstances to the current insurer before the expiry date of that insurance*.

It does not matter at all when the act, error or omission that may have given rise to the claim or potential claim may have occurred; *only that the Insured had no prior knowledge of the circumstances before taking up the cover*. This rule is subject to the provision that there is no retroactive date limitation in the policy. If there is, then the policy will not respond to acts, errors or omissions that occurred prior to the date the insurance commenced.

The Legislation Affecting Insurance in New Zealand

There are a number of statutes and regulations that regulate the New Zealand insurance industry and touch on engineering activity. Some of the more significant acts are as follows:

- *The Insurance Companies' Deposits Act 1953* requires every company or person carrying on any class of insurance business to deposit $500,000 as a security with the Public Trustee.
- *The Insurance Law Reform Acts 1977* and *1985* improve the position of the insured under any contract of insurance and are intended to improve the balance and bargaining power between the insurer and insured.
- *The Earthquake Commission Act 1993* provides compulsory earthquake and certain natural disaster coverage for residential homes and their contents that are otherwise insured for fire up to maximum limits.
- *The Insurance Companies' (Ratings & Inspections) Act 1994* requires insurers (other than certain exempted insurers who do not underwrite disaster or general insurance) to obtain a rating from an approved rating agency to be disclosed at the time of entering into or renewing a contract of insurance.
- *The Accident Insurance Act 1998* provides for compulsory private insurance in respect of accidental bodily injury. The Act has since been amended to remove private insurance competition with effect from 1 July 2000 and to reintroduce a single statutory compulsory regime.

Insurance Requirements

The law requires an insured to act as a reasonable and prudent uninsured person *and to mitigate the circumstances of any loss*. This precept excludes reckless salvage claims in the case of a material damage claim, or recklessly compromising the insured's, and thus the insurer's position in a liability claim.

In the case of liability policies, the point is further emphasised by spelling out in the policy that *the insured must make no admission of liability*, even if the insured believes that they are liable in any event for which insurance cover has been taken.

References

1 Adam, D F (1984): "Insurance for engineers and engineering works". In *"Engineering Risk"*, IPENZ, Wellington, pp 84-88.

2 Hammond, J D (1980): "Risk-spreading through underwriting and the insurance institution". In Schwing, R C and Albers, W A (ed.) "*Societal Risk Assessment: How Safe is Safe Enough?"*, pp 147-148, Plenum Press, New York & London.

Complete List of References

Adam, D F (1974): "Insurance for engineers & engineeering works", in "*Engineering Risk*", 84-88, IPENZ, Wellington.

Anyakora, S N, Engel, G F M and Lees F P (1971): "Some data on the reliability of instruments in the chemcial plant environment", *Chem. Engr.* No. 255, 396.

AS/NZS 3931:1995: "*Risk Analysis of Technological Systems*." Standards Australia & Standards New Zealand, Homebush & Wellington.

AS/NZS 4360:1999: "*Risk Management*", Standards Australia & Standards New Zealand, Homebush & Wellington.

Atomic Energy Commission (1975): "*Reactor Safety Study: An Assessment of Accident Risks in US Commercial Nuclear Reactors*", Rep. WASH-1400, Washington, DC.

Baker, A R (1976): "*Accident Investigation*", Dept Chem. Eng., Loughborough Univ., reported by Lees (1996).

Bennet, A J (1992): *"Rapid ranking of process hazards*", unpublished, Chem. and Proc. Eng., Univ. Canterbury, Christchurch, reported by Sanders (1992).

Blackmore, G A and Shannon, H D (1996): "Risk-based safety-management auditing", *Process Safety and Environ. Protection*, *74*(B1), 38-44.

Bond, J (1996): "*The Hazards of Life and All That*", Inst. Physics, Bristol.

Boyes, W J (1998): *"Risk assessment for a port proposed at Marsden Point by Northland Port Corporation"*, BE (Chem. & Proc.) Rep., Univ. Canterbury, Christchurch.

Bowen, J H (1976): "Individual risk vs public risk criteria", *Chem. Eng. Prog. 72* (2), 63.

Bretherick, L (1990): *"Bretherick's Handbook of Reactive Chemical Hazards*", 4th edn, Butterworth Heinemann, London.

Bryan, J L (1976): "The determination of behavior responses exhibited in fire situations", *J. Fire Flammability*, *7*, 319.

Carson, P A and Mumford, C J (1986): *Loss Prevention Bull.* No.067, IChemE, Rugby.

Carter, R P (1999): "*Risk and Prudence: IPENZ Policy on Engineering Governance in Public and Private Organisations*", IPENZ, Wellington.

Chemical Engineer, The (1998): "Power-cut hits Dounreay", 14 May, 5.

Christchurch Engineering Lifelines Group (1997): "*Risks and Realities*", CAE, University of Canterbury, Christchurch.

Cothern, C R , Coniglo, W A and Marcus, W L (1986): "Estimating risk to human health", *Environ. Sci. Technol.*, *20*(2), 111-116.

Crossland, B et al. (1992): Estimating engineering risk, in "*Risk: Analysis, Perception and Management*", 13-34, Royal Society, London.

Cullen, the Hon. Lord (1990). *"The Public Inquiry into the Piper Alpha Disaster"*, HMSO, London.

Dunster, H J and Vinck, W (1979): "The assessment of risk - its value and limitations", *Eur. Nuclear Conf. Foratom VII Cong. Hamburg*, 162-166, Vulkan-Verlag, Essen. [reported by Crossland et al. (1992)].

Eisenberg, N A, Lynch, C J and Breeding, R J (1975): "*Vulnerability Model: A Simulation System for Assessing Damage from Marine Spills*", Rep. CG-D-136-75, Enviro Control Inc, Rockville MD.

Elms, D G (1992): "Risk assessment" in D J Blockley (ed.) "*Engineering Safety*", McGraw-Hill, New York.

Elms, D G (1998): "Overview - Prudence, principles and practice", in Elms D (ed.) "*Owning the Future: Integrated Risk Management in Practice*", CAE, University of Canterbury,Christchurch.

Environmental Risk Managment Authority (1998): "*Methodology for the Consideration of Applications for Hazardous Substances and New Organisms under the HSNO Act 1996*", Final proposal Jan. 1998, ERMA New Zealand, Wellington.

Farmer, F R (1981): "Quantification of physical and engineering risks", *Proc. Roy. Soc. London, A 376*, 103-119.

Fell and Hartford (1997). Reported in *BRANZ Study Report No 83*, 1999.

Ferguson, G and Andow, P K (1986): "Process plant safety and artificial intelligence", *Proc. World Cong. III Chem. Engng*, Tokyo, 1092.

Findlay, P J, Mostyn, G R and Fell, R (1997): *Vunerability to Landsliding*, reported by Riddolls and Grocott Ltd (1999).

Frijling, J K (1993): "Probabilistisch ontwerpen" (probabilistic projects), *Proc. Applied Risk Symp.*, Royal Netherlands Institution of Engineers, Den Haag.

Fussell. J B (1976): "Fault tree analysis: concepts and techniques", in Henley, E J and Lynn, J W (eds) "*Generic Techniques in Systems Reliability*", p 135, Noordhoff, Leyden.l

Fussell, J B and Kumamoto (1976). "*Reliability Engineering and Risk*

Assessment", Prentice Hall, New York.

Gardenier, J (1992): "General concepts of risk", in Gardenier, J and Keey, R B (ed.) "*Risk Assessment of Natural and Industrial Hazards*", 11-32, CAE, University of Canterbury, Christchurch.

Gardenier, J (1993): *Report on nuclear powered ships. A credible proof of negligible risk?*, (unpublished), Wellington.

Gillett, J (1985): "Rapid ranking of hazards", *Proc. Engng*, Feb. 19.

Gordon, C (1999): "Project finance can increase engineering risk", *NZ Eng* 54(2),28-9.

Gough J D (1988): *"Risk and Uncertainty"*, Inform. Paper, no. 10, Centre for Resource Management, Univ. Canterbury & Lincoln College.

Gough, J D (1990): "A review of the literature pertaining to 'perceived' risk and 'acceptable' risk and the methods used to estimate them", *Inform. Paper no. 14*, Centre for Resource Management, Lincoln.

Hammond, J D (1980): "Risk-spreading through underwrting and the insurance institution", in Schwing, R C and Albers, W A, Jnr (ed.) "*Societal Risk Assessment. How Safe is Safe Enough?*", 147-178, Plenum Press, New York London.

Haness, S J and Warwick, J J (1991): "Evaluating the hazard ranking system", *J. Environ. Management*, *32*, 165-176.

Hayward, J A (1982) in Keey, R B et. al. *"Engineering and Society"*, Univ. of Canterbury publ. No. 31.

Health and Safety Commission (1991): "*Major Hazard Aspects of the Transport of Dangerous Substances*", HMSO, London.

Health and Safety Executive (1988): "*The Tolerability of Risks from Nuclear Power Stations*", HMSO, London.

Health and Safety Executive (1989): *"Risk Criteria for Land-use Planning in the Vicinity of Major Industrial Hazards"*, HMSO, London.

Helm, P (1997): "Risk assessment, methodology, vulnerability, impact and importance", in *Rep. Christchurch Engineering Lifelines Group: "Risks & Realities"*, CAE, Univ. Canterbury, Christchurch.

Hill, E J and Bose, L J (1975): "Sneak circuit analysis of military systems", *Proc. 2nd Internat. Systems Safety Conf.*, 351- 372 [reported by Whetton (1993)].

Hom, S and Ellis, M (1998): "A framework for manging risks associated with human-induced hazards", in Elms, D (ed.) "*Owing the Future. Integrated Risk Management in Practice*", pp 227-240, CAE, University of Canterbury, Christchurch.

Hynes, M and Vanmarke,E (1976): "Reliability of embankment performance prediction", in *Proc. ASCE Engng Mechanic Div. Conf.*, Waterloo, Ontario, Univ. of Waterloo Press [reported by Pidgeon et al.(1992)].

Iliffe, R E, Chung, P W H and Kletz, T A (1999): "More effective permit-to-work systems", *Proc. Safety & Environ. Protection*, 77(B2), 69-73.

Kasper, RE et al. (1998): "The social amplification of risk", *Risk Anal. 8*(3), 435-455.

Kates, R W and Kasperson, J X (1983): "Comparative risk anlysis of technological hazards", *Proc. Nat, Acad. Sci*. USA, 80, 7027-7038.

Keey, R B (1986): "The use of hazard-warning analysis", *Chem. Eng. Process*., *26*, 289-296.

Keey, R B (1987): "*Reliability in the Process Industries*", IPENZ, Wellington.

Keey, R B (1991): "A rapid hazard-assessment method for smaller-scale industries", *Proc. Safety & Environ. Protection*, *69*(B2), 85-89.

Keey, R B and Smith, C H (1984): "The propagation of uncertainties in failure events", *Reliab. Engng*, *10*, 105.

Khan, A R and Hunt, A (1989): "The propagation of fualts in process plants: integration of fault propagation technology into computer-aided design", *IChemE Symp. Ser*. No. 114, 35-43.

Kinsman, P (1991): "*Major Hazard Assessment: A Survey of Current Methodology and Information Sources*", HSE Rep. No. 29, UK Health and Safety Exec., London

Kletz, T A (1971): "Hazard analysis - A quantitative approach to safety", *IChemE Symp. Ser*., No. 34, 75-81.

Kletz, T A (1985): "Estimating potential hazards", *Chem. Eng*., 1 April, 48-68.

Kletz, T A (1995): "Improving organisations' memories", *IChemE Loss Prevent. Bull*. No.124, 20-1.

Kletz, T A (1999): "*Hazop and Hazan*", 4th edn, IChemE Rugby, UK.

Knowlton, R E (1981): "*An Introduction to Hazard and Operability Studies: The Guide Word Approach*", Chemetics International Ltd, Vancouver, BC

Landon-Jones, I, Wellington, N B and Bell, G (1995): *"Risk assessment of Prospect Dam"*, IPENZ Proc. Techn. Groups 21/1 (LD), 55.

Lardner, R, Miles, R and Flemming, M (2000). "Safer behaviour at work", *Chem. Eng*., No. 694, 23.

Leathley, B and Nicholls, D (1998): "Imroving the effectivenes of Hazop: a

psychological approach", *IChemE Loss Prevention Bull*., no. 139, 8-11.

Lee, T R (1981): "Perception of risk: the public's perception of risk and the question of irrationality", *Proc. Roy. Soc. London*, A 376, 5-16.

Lees, F P (1996): "*Loss Prevention in the Process Industries*", 2nd edn, Butterworth-Heinemann, London.

Liquid Fuels Trust Board (1984): *"Risk Assessment of Future LPG Facilities in New Zealand"*, Rep. No. LF 5006, LFTB, Wellington.

Lowrance, W W (1976): "*Of Acceptable Risk*", W Kaufmann, Los Altos, CA.

Lucas, D (1997): "The causes of human error", in Remill, F and Rajan, J, "*Human Factors in Safety-critical Systems*", Butterworth Heinemann, Oxford.

MacKenzie, A D (1984): "The legal responsibility of engineers", in "*Engineering Risk*", 71-83, IPENZ, Wellington.

McKay, G. (1999): "Designing a process hazards analysis methodology for a "non-traditional" chemical facility", *IChemE Loss Prevention Bull*. No 147, 22-6.

McNamee, D and Selim, G (1998): "Risk management: Changing the inernal auditor's paradigm", *Inst. Internal Auditors Res. Found*., Altamonte Springs, FL.

Mahoney, D G (ed)(1990): *"Large Property Damage Losses in the Hydrocarbon-chemical Industries"*, 30th edn., M&M Protection Consultants, New York

Merrison, A W (1971): *"Inquiry into the basis of design and method of erection of steel box girder bridges"*, HMSO, London.

Newby, H (1997): "Risk analysis and risk perception: The social limits of technological change", *Proc. Safety & Environ. Protection*, 75 (B3), 133-7.

Newnham, W L (1971): "*Learning Service Achievment. Fifty Years of Engineering in New Zealand*", NZIE, Wellington.

NZS 4801(Int):1999: *"Occupational Health and Safety Managment Systems, Specifications with Guidance for Use"*, Standards NZ, Wellington .

O'Mara, R L and Bergeron, C B (1987). "Inherent safety - how to keep a new safety system from causing an accident", cited by Kletz, T A (1999), "*Hazop and Hazan*", 4th edn. IChemE, Rugby, UK.

Palmer, E R (1990): "Town planning criteria for operations with hazardous chemicals", *Proc. Annual Conf. IPENZ Wellington*, II, 73-84.

Parmar, J C and Lees F P (1987): "The propagation of faults in process

plants: hazard identification", *Reliability Engng*, *17*(4), 277.

Pavolic, K. (1983): "Autonomy and obligation: is there an engineering ethic", in Schaub, J H and Pavolic, K ed., "*Engineering Professionalism and Ethics*", Wiley, New York, 223-232.

Peet, W and Ryan, R (1998): "Risk managment in a network operation: understanding complex systems", in Elms D G (ed.)"*Owning the Future: Integrated Risk Management in Practice*", CAE, University of Canterbury, Christchurch.

Pidgeon, N, Hood, C, Jones, D, Turner, B and Gibson, R (1992): "Risk perception", in "*Risk: Analysis, Perception and Management*", 89-134, Royal Society, London.

Pikaar, M J and Seaman, M A (1995): *"A review of risk control"*, Rep. SVS 27A, VROM, Den Haag.

Pinkus, R L B, Shuman, L J, Hummon, N P and Wolfe, H (1997). "*Engineering Ethics: Balancing Cost, Schedule and Risk*", Cambridge UP, Cambridge.

Pollard, D (1998): "How safe is safe enough?", *NZ Eng*. *53*(5), 30-1.

Powell, L (1995): *"Explosion risk analysis for valve-vented storage water heaters"*, BE (Chem.& Proc.) Rep., Univ. Canterbury, Christchurch.

President's Task Committee on Professional Practice & Risk (1984): "*Engineering Risk*", IPENZ, Wellington.

Provinciale Waterstaat Groningen (1979): *"Pollution control and use of norms in Groningen"* (Nota millieunormen provincie Groningen), PW Groningen.

Riddolls & Grocott Ltd (1999): "*Quantitative Risk Assessment Method, for Determining Slope Stability in the Building Industry*", BRANZ Study Rep. No.83, BRANZ Porirua.

Robens, Lord (1972): "*Safety and Health at Work*", Cmnd 5034, HMSO, London.

Rothchild, Lord (1978): "Risk", *The Listener*, 100, 715.

Rutstein, R and Clarke, M B T (1979): "Probability of fire in different sectors of industry", *Fire Surveyor*, 8(1), 20.

Sabey, B E and Taylor, H (1980): "The known risks we run: the highway", in Schwing, R C and Albers, W A Jnr (eds), "*Societal Risk Assessment: How Safe is Safe Enough*.", 43-70, Plenum Press, New York London.

Sanders, K A (1992): *"Production and evaluation of safety assurance software for process industrial sites in New Zealand"*, ME thesis, Chem. and Proc. Eng., Univ. Canterbury Christchurch.

Sax, N I (1989): "*Dangerous Properties of Materials*", 7th edn, van Nostrand Reinhold, New York.

Sherwin, D J and Lees, F P (1980). "An investigation of the application of failure data analysis to decision-making in maintenance of process plants", *Proc. IMechE, 194*, 301, 308.

Skelton, B (1997). "*Process Safety Analysis - An Introduction*", IChemE, Rugby, UK

Slater, D H, Corran, E R, Pitblado, R M (1986): "*Major Industrial Hazards*", Project Rep., Warren Centre, Univ. Sydney NSW.

Slovic, P, Fischoff, B and Lichtenstein, S (1981): "Perceived risk: psychological factors and social implications", *Proc. Roy. Soc. London, A 376*, 17-34.

Smith, D J (1993): "*Reliability Maintainability and Risk*", 4th edn, Butterworth-Heinemann, Oxford.

Smith, M (1998): "Safety can be fun", *IChemE Loss Prevention Bull.*, No. 139, 2.

Special Committee on Nuclear Propulsion (1992): "*The Safety of Nuclear Powered Ships*", Dept of the Prime Minister and Cabinet, Wellington.

Stallen, P J M, Geerts, R and Vrijling, H K (1996): "Three conceptions of quantified societal risk", *Risk Analysis*, *16*, 635-643.

Stern, P C and Fineberg, H V (eds)(1996). "Understanding Risk", *"Informing Decisions in a Democratic Society"*, Nat. Acad. Press, Washington, DC

Stewart, J C (1994): *"Risk assessment of natural and industrial hazards"*, BE Rep., Chem. and Proc. Eng., Univ. Canterbury, Christchurch.

Suter, G W (1993): "*Ecological Risk Assessment*", Lewis, Chelsea MI.

Taylor, J R, Kampmann, J, Kragh, E K, Becher, P and Petersen, K E (1989): "*Quantitative and Qualitative Risk Criteria for Risk Acceptanc*e", Rep. Miljøstrelsen, ITSA, Roskilde, DK.

Treeweek, D N, Calydon, C R and Seaton, W H (1973): "Appraising energy hazard potentials", *Loss Prevention*, *7*, 21.

Tuli, R W and Apostolakis, G E (1996): "Incorporating organizational issues into root-cause analysis", *Process Safety & Environ. Protection*, *74*(B1), 3-16.

Turner, K A and Shuster , R L (1996). "Landslides: investigation and mitigation", *Trans. Res. Board Special Pub. Rep. 247*, reported in BRANZ Study Report No. 83, 1999

Tweeddale, H M (1992): "Balancing quantiative and non-quantitative risk

assessment", *Process Safety and Environ. Protection*, *70*(B2), 70-74.

Walker, I K (1981): "*Occupational Safety*", State Services Commission, Wellington.

Wallace, I G (1995): "*Developing Effective Safety Systems*," IChemE, Rugby, UK.

Watson, J (1998): "Consultation - law & possibility", *N.Z. Eng.*, *53/5*, 7-8.

Wells, G (1996):"*Hazard Identification and Risk Assessment*", IChemE, Rugby, UK

Wells, G (1997): "*Major Hazards and Their Managemen*t", IChemE, Rugby, UK

Whetton, C P (1993): "Sneak analysis of process systems", *Process Safety and Environ. Protection*, *71*(B3), 169-179.

Wood, S and Tweeddale, H M (1990): "Rosebank Peninsula risk assessment study - A review of safety and risks in an Auckland industrial area", *Proc. Annual Conf. IPENZ Auckland*, II, 51-61.

Zach, L S and Keey, R B (1995): "Towards a methodology for environmental risk analysis", in Melchers, R E and Stewart, M G (eds) "*Integrated Risk Management*", 235-242, Balkema, Rotterdam.

Zach, L S and Keey, R B (1998): "Risk analysis of chemical contaminants in the environment: estimating the long-term consequences from frequent low-level accidents", *Proc. Conf. Environ. Strategies for 21st Century*, Singapore.

Appendix A: Fault-tree Development

The reduction of a fault tree to the minimum sequence of events may be done by Fusell's algorithmn, which is particularly attractive for this purpose, as the methodology can be adapted to a spreadsheet representation for hand or computer-aided evaluation.

The rules can be stated as follows:

AND-gate rule

- The first input replaces the higher-order event.
- Other inputs are inserted in the next available column, one input per column.

OR-gate rule

- The first input replaces the higher-order event.
- The other inputs are inserted into the next available row, one input per row.
- If there are other entries in the row where the OR gate appears, these must be entered into the next row.

This procedure is illustrated for the simple fault tree for the overheating of an electric motor, which may be due to either a primary motor failure or to excessive current (Figure A1).

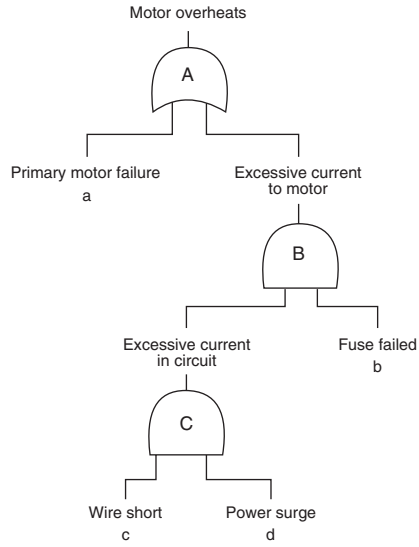


Figure A1: Fault tree for a motor-system failure (after Fussell, 1976)

The steps are:

Step 1. Insert the top-event gate:

A

Step 2. Replace A (an OR gate) with its inputs, a and B:

a

B

Step 3. Replace B (an AND gate) with its inputs, C and b:

a

C b

Step 4. Replace C (an AND gate) with its inputs c and d:

a

c b

d b

The minimum cut sets are thus: a; c b; and d b.

Fussell's method may also be used to eliminate unnecessary sets in an unreduced fault tree. Consider the fault tree shown in Figure A2(a), in which the same event b, say the failure of manual intervention, is found in separate branches. The final spreadsheet would have the sets:

a b b

a d b

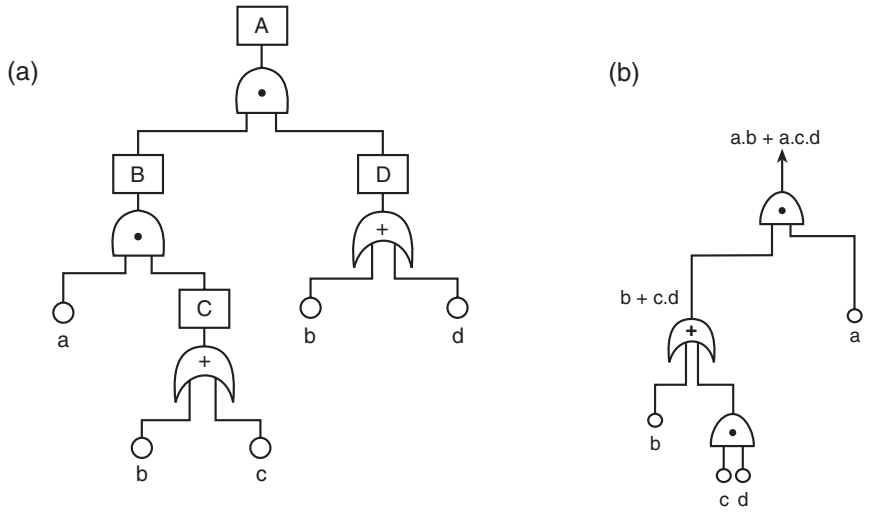
a b c

a d c

In the first row, there is a repeated event b which can be deleted. The second and third rows can be deleted since these are supersets of a,b. The minimum cut sets are thus a,b and a,d,c. This leads to the reduced fault-tree depicted in Figure A2(b).

Boolean reduction gives A = a•b + a•c•d, revealing that the minimum cut sets are indeed a,b and a,d,c.

By inserting values for the primary probabilities it can be shown that the unreduced fault tree substantially underestimates the outcome probability.



Boolean reduction

A = B•D
= (a•C) • (b + d)
= (a•(b + c)) • (b + d)
= a • (b + c) •b + a•(b + c) •d
= {[(a + b) + (a•b)•c] + {a•b]•d} + a•c•d
= {[a•b] + [a•b]•d} + a•c•d
= a•b + a•c•d

Figure A2: (a) Unreduced (b) reduced fault tree

For example, let a = 0.2, b = 0.1, c = 0.05 and d = 0.1. The unreduced fault tree, Figure A2(a) yields:

$$C = b + c = 0.1 + 0.05 = 0.15$$

$$B = a \bullet c = 0.2 \times 0.15 = 0.03$$

$$D = b + d = 0.1 + 0.1 = 0.2$$

$$A = B \bullet D = 0.03 \times 0.2 = 0.006$$

Whereas the reduced fault tree, Figure A2(b), gives:

$$A = a \bullet b + a \bullet c \bullet d$$

$$= (0.2 \times 0.1) + (0.2 \times 0.05 \times 0.1) = 0.021$$

which is 3.5 times greater! For simplicity, the small probabilities of simultaneous inputs to OR-gates have been neglected.

Reference

Fussell. J B (1976): "Fault tree analysis: concepts and techniques", in Henley, E J and Lynn, J W (eds) "*Generic Techniques in Systems Reliability*", p 135, Noordhoff, Leyden.

Appendix B: Risk and Prudence

Engineering Governance in Public and Private Organisations

IPENZ Recommendations for the Prudent Management of Engineering Activities in Public Companies, Local Authorities and Crown Agencies.

Introduction

The Institution of Professional Engineers New Zealand (IPENZ) is the professional body representing engineers and technologists in New Zealand. It has produced these guidelines to assist directors, councillors, and executive managers in public companies, crown agencies and territorial local authorities with the prudent management of their engineering assets and operations.

Rationale

Adherence with this policy will assist directors and executive management, and those with statutory responsibilities for compliance with the legislative requirements[1], to show that they have acted prudently and have followed "best practice" in setting up appropriate processes and accountabilities. Compliance with this policy will also assist in ensuring that engineering activities are managed in support of the broader business activities.

Applicability

These guidelines are designed for public companies, crown entities, government bodies and territorial local authorities which **either**

(i) Rely intensively on engineering and technology to deliver or produce their services and products;

or

(ii) Engineering-related risks are a significant proportion of the total business risk.

Board Positions

Organisations should ideally have at least one Board Member with a recognised professional engineering background[2]. That person will, in addition to their normal Board responsibilities, be expected to add an engineering and tech-

nology perspective to Board policy making. The Board should also recognise that it may need to take advice on engineering matters from both within the company and from external sources.

Executive Management

Such organisations should have:-

(i) A person or persons (as appropriate) with clear responsibility and accountability for engineering and technology matters. This person should be eligible for professional membership of a recognised engineering institution.

The position description should include responsibility for ensuring that:-

(i) The engineering and technology policies are embodied within the business policy and strategies.

(ii) Engineering risks are properly evaluated and considered in evaluating business risk.

(iii) The engineering and technology applied in the businesses meet 'best practice' guidelines.

Business Processes

The organisation should have within its strategic business processes:-

(i) A regular performance audit of its engineering policies (including human resource policies applying to engineering personnel) against industry 'best practice'.

(ii) An engineering risk evaluation programme

Conclusion

Adherence to this policy will assist those with governance responsibilities to show that they have acted prudently in managing the engineering resources entrusted to them.

R P Carter KNZM

President

References

1 Commerce Act, Health and Safety in Employment Act

2 Professional Engineering Background

For purposes of this document a person described as having a professional engineering background is one who is eligible for membership of a recognised professional engineering institution. Such people are required to have a tertiary qualification (Bachelor of Engineering (BE) or equivalent) and at least four years post graduation experience. This experience is assessed by senior engineers through interviews, submitted work and referees reports before entry into the class of Member (M.IPENZ) is granted.

Engineering Institutions recognised in New Zealand are; IPENZ (Institution of Professional Engineers New Zealand), IE Aust (Institution of Engineers Australia), IEE (Institution of Electrical Engineers), IMechE (Institution of Mechanical Engineers), IChemE (Institution of Chemical Engineers), ICE (Institution of Civil Engineers), IStructE (Institution of Structural Engineers), and HKIE (the Hong Kong Institution of Engineers).

These people are generally identified by a post-nominal, e.g. M.IPENZ and F.IPENZ.

Appendix C: Information on CAE

CAE, the Centre for Advanced Engineering, was established in May 1987, as a centre for the promotion of innovation and excellence in engineering and technology, to commemorate the centenary of the School of Engineering at the University of Canterbury.

Vision Statement

To benefit New Zealand through promoting and encouraging the application of advanced engineering and technology.

Objective

CAE aims to enhance engineering knowledge within New Zealand by technology transfer and the application of New Zealand and overseas research to engineering-related issues of national importance.

Key Activities

- CAE undertakes major projects that bring together selected groups of practising and research engineers and other experts from industry, research organisations, local and central government, tertiary institutions, and the engineering profession.
- CAE also carries out smaller projects and organises seminars, workshops and conferences as opportunities arise.

CAE projects aim to:

- Be of national importance with wide public appeal and with tangible results.
- Facilitate technological co-operation amongst commercial and government organisations, tertiary institutions and the engineering profession.
- Identify deficiencies in New Zealand's technological capability and take action to promote the addressing of these deficiencies.
- Undertake technology transfer rather than original research.

Funding

CAE is an independent, non-profit organisation, financed mainly from the earnings of its trust fund. This fund, which currently stands at approximately $2.3

million, consists of monies donated initially by 150 corporate donors and 750 individual donors during the 1987 Centennial Appeal, and more recently supplemented by further donations during the 10th Anniversary Appeal. Other income is derived from sponsorship for specific projects, book sales and seminars. The University of Canterbury continues to make a major contribution to CAE by providing accommodation and financial services.

Administration

CAE is controlled by a Board of Directors comprising representatives from industry and commerce (including government and consulting engineers), the University of Canterbury and other tertiary educational institutions. The present Chairman is Dr Francis Small of Wellington. The Trust Fund is currently administered by the University of Canterbury under the direction of four trustees. CAE has two executive staff and three other staff engaged on publications and secretarial duties.

Executive Director John Blakeley has overall responsibility for CAE activities and Projects Director John Lumsden co-ordinates CAE projects. From 1 May 2000, Dr George Hooper succeeds John Blakeley as Executive Director.

Principal Corporate Donors

Founders:

BHP New Zealand Steel Limited
Earthquake Commission
Electricity Corporation of New Zealand
Fisher & Paykel Industries Limited
Mainzeal Property and Construction Limited
McDonnell Dowell Constructors Limited
Opus International Consultants Limited
TransAlta New Zealand Limited

10th Anniversary Appeal:

Transpower New Zealand Limited

Contact:

CAE
University of Canterbury
Private Bag 4800
Christchurch, New Zealand

Street Address:

39 Creyke Road
Christchurch 8004

Telephone: +64-3-364-2478
Fax: +64-3-364-2069
e-mail: cae@cae.canterbury.ac.nz
http://www.cae.canterbury.ac.nz

Executive Director: John P Blakeley (to 30 April 2000)
Dr George Hooper (from 1 May 2000)

Projects Director: John L Lumsden

Publications Editor: Charles A Hendtlass

Appendix D: Information on IPENZ

The Institution of Professional Engineers New Zealand sets the standards for professional engineering in New Zealand. It does this through accrediting undergraduate engineering degrees and assessing practice competency of individuals through professional review. By participating in international engineering agreements, IPENZ ensures that New Zealand professional engineering qualifications are recognised throughout the world.

The Institution's Code of Ethics imposes standards of conduct covering professionalism and integrity, society and community wellbeing, sustainable management and promotion of engineering knowledge. The Code, which is backed up by a disciplinary process gives assurance to the public and clients that members will act in a competent and professional manner.

IPENZ recognises the duty of the profession to promote engineering to the young generation of New Zealanders. To achieve this it has developed its Neighbourhood Engineers Programme which brings together engineers and schools as part of the new Technology Curriculum.

By advocating and promoting engineering to the government, industry and the community, IPENZ assists in providing an environment where engineers can practice their profession with identity, respect and rewards.

The Institution offers its members:

- Various awards and scholarships that recognise engineering excellence and innovation.
- Quality brand identification through the use of post nominals M.IPENZ, T.IPENZ.
- A weekly e-mail magazine that provides members with up-to-the-minute news and events.
- A web site provides comprehensive information on activities, resources and information.
- The peer-reviewed Transactions of the best technical papers on engineering in New Zealand.
- Status and recognition as someone who meets strict codes of competency and ethics. Increasingly sought by employers, this improves employment or

career advancement prospects.

- Assistance in keeping up to date via "e.nz" delivered to all members every second month. This magazine provides a blend of news and feature stories of interest to engineers practising across a broad spectrum of disciplines, together with the latest on what IPENZ is doing for its members.
- Mutual Recognition Agreements with numerous engineering bodies overseas assist in obtaining recognition for work overseas or to operate in a company which provides international services.
- An annual remuneration survey provides information on salary packages for engineers and technologists in a wide range of disciplines, locations, jobs and speciality areas.
- Over twenty special interest groups provide a range of services including meetings, publications and practice standards.
- A network of professional contacts through local Branch and Technical Group meetings and activities with opportunities to meet and exchange information, experience and ideas.
- An employment advisory service providing information on employment conditions and contracts.
- Through an e-mail system, members can access a job search list where job vacancies are advertised. Students can also use a similar system for identifying those organisations offering holiday employment.
- Assistance and monitoring of Continuing Professional Development to maintain skills. This is supported by IPENZ in being the link for the Deakin University MBA programme, listing available conferences and courses in the "e.nz" magazine, collating lists of relevant programmes, evaluating and endorsing courses, arranging mentors, giving career advice, and providing articulated pathways.
- Career/competency programmes to assist young engineers in planning and tracking their career development under the guidance of an experienced engineer, with National Office support.
- An employer endorsement programme to recognise organisations that have systems in place to support young engineers in their career development.
- Assistance from the Benevolent Society in time of need is available to both members and their families.

Mission Statement

The Institution of Professional Engineers New Zealand is dedicated to enhancing the quality of life by the creative application of engineering and technology.

For the Community we will:

- advance the practice of engineering and technology
- promote sustainable management of the environment

For our Clients we will:

- determine and encourage high standards
- sustain these with ethics and discipline
- assure the qualifications of our members
- encourage innovative solutions.

For our Colleagues we will:

- facilitate the acquisition and sharing of knowledge
- represent their interests.

We aim to be the organisation which is the first choice for membership by all people who through study, qualifications, work or general interest share in this dedication.

To Contact IPENZ

E-mail and Internet

ipenz@ipenz.org.nz
www.ipenz.org.nz

Postal

P O Box 12 241
Wellington 6004
New Zealand

Telephone and Facsimile

(64) 4 473 9444 (phone)
(64) 4 473 2324 (fax)

Index

F

G

H

I

L

M

S

T

U

V

W

MANAGEMENT OF ENGINEERING RISK

The aim of this book, a joint publication of the Institution of Professional Engineers New Zealand (IPENZ) and the Centre for Advanced Engineering (CAE), is to provide an overview of the strategy and techniques of engineering-risk management.

There are a large number of books available which deal with engineering risk analysis and the calculation of reliability, but almost none that describe these activities within the wider context of managing risk in technological enterprises. It is hoped that this particular book will go some way towards filling that gap.

The book has its origins in a 1983/84 IPENZ publication on Engineering Risk and the initial objective was to update that publication, but the focus subsequently changed towards the management of risk within engineering organisations. Some recent major incidents in both New Zealand and Australia have emphasised to many practising engineers the importance of implementing appropriate risk-management procedures on projects for which they are responsible.

The publication of a generic Australian/New Zealand Standard on Risk Management (AS/NZS 4360:1995) and its reissue in revised form in 1999 have also been an influencing factor in the preparation of this book.

It is hoped that the book will be useful to members of the engineering profession and other people associated with engineering activities wishing to implement a risk-management approach within their own organisation or project, both as a "companion volume" in providing an introduction to the application of AS/NZS 4360:1999, and other standards; and as a first guide to engineering risk, its perception, identification and evaluation, which forms a basis for the prudent management of engineering assets and operations.

ISBN 0-908993-25-0